AALTO UNIVERSITY
School of Science
Department of Computer Science

ELEMENTS OF TRUST AND THEIR IMPACT ON PURCHASE INTENTION AND CUSTOMER LOYALTY OF ONLINE SERVICE USERS – CYBERSECURITY PERSPECTIVE

Miska Laakkonen

Master's Thesis
Espoo, November 20, 2017

Supervisor and instructor: Professor Antti Ylä-Jääski

AALTO UNIVERSITY
School of Science
Department of Computer Science

Abstract of
Master's thesis

Author:	Miska Laakkonen		
Title:	Elements of trust and their impact on purchase intention and customer loyalty of online service users – cybersecurity perspective		
Date:	November 20, 2017	**Pages:**	6 + 56 + 10
Professorship:	Data Communications Software	**Code:**	T-110
Supervisor:	Professor Antti Ylä-Jääski		
Instructor:	Professor Antti Ylä-Jääski		

Online commerce is growing rapidly, and the increasing competition forces online service providers to find ways to differentiate their online service from competition in order to get potential customers to purchase from their online service instead of competing online services. Trust has been found as a significant factor that influences initial purchase decision and customer loyalty of online service users, and therefore provides service providers one way to differentiate from competition.

This study examines existing research that links online trust to purchase intention and customer loyalty, and describes the factors that contribute to the online trust. Based on existing literature, a research model is developed to study individual elements of online trust and their impact on purchase intention and customer loyalty. Based on the research model a survey is conducted to find out how different scenarios related to privacy, security, reputation and usability of online service, influence perceived online trust.

Findings of this study demonstrate that transparency and control over personal information have a positive impact on online trust, and describes scenarios that increase perceived security and thus increase online trust. Findings of the study also point out the negative impact of data breach disclosures on online service's reputation, which in turn decreases online trust towards the online service, and demonstrate the easy-to-use authentication increases online trust whereas decreased availability of online service negatively impact online trust.

Keywords:	Online Trust, Online Services, Digital Services, e-Commerce, Consumer Behaviour, Privacy, Security
Language:	English

AALTO-YLIOPISTO
Perustieteiden korkeakoulu
Tietotekniikan laitos

Diplomityön tiivistelmä

Tekijä:	Miska Laakkonen		
Työn nimi:	Luottamuksen elementit, ja niiden vaikutus verkkopalveluiden käyttäjien ostoaikeeseen ja asiakasuskollisuuteen – tietoturvanäkökulma		
Päivämäärä:	20. marraskuuta 2017	**Sivuja:**	6 + 56 + 10
Professuuri:	Tietoliikenneohjelmistot	**Koodi:**	T-110
Valvoja:	Professori Antti Ylä-Jääski		
Ohjaaja:	Professori Antti Ylä-Jääski		

Verkkoliiketoiminta kasvaa nopeasti, ja kasvanut kilpailu pakottaa verkkopalveluiden tarjoajat differoimaan verkkopalvelunsa suhteessa kilpailijoihinsa saadakseen potentiaaliset asiakkaat ostamaan heidän verkkopalvelustaan kilpailevien verkkopalveluiden sijasta. Verkkopalvelua kohtaan tunnetun luottamuksen on todettu vaikuttavan merkittävästi verkkopalveluiden käyttäjien ensimmäiseen ostopäätökseen sekä asiakasuskollisuuteen, mikä antaa palveluntarjoajille yhden keinon differoida verkkopalvelunsa suhteessa kilpailijoihin.

Tämä työ tekee kirjallisuuskatsauksen tutkimuksiin, jotka osoittavat luottamuksen ja ostoaikeen sekä asiakasuskollisuuden välisen yhteyden, sekä käsittelevät tekijöitä jotka vaikuttavat luottamukseen. Katselmoitujen tutkimusten perusteella esitellään tutkimusmalli, joka on kehitetty tätä työtä varten yksittäisten luottamukseen - ja sitä kautta ostoaikeeseen ja asiakasuskollisuuteen - vaikuttavien tekijöiden tutkimiseen. Kehitetyn mallin perusteella työtä varten suoritettiin kyselytutkimus, jolla selvitettiin, miten erityyppiset verkkopalvelun yksityisyydensuojaan, tietoturvaan, maineeseen ja käytettävyyteen liittyvät skenaariot vaikuttavat käyttäjien kokemaan luottamukseen.

Tämän työn tulokset osoittavat, että läpinäkyvyys sekä mahdollisuus hallita omien henkilötietojen käyttöä vaikuttavat myönteisesti käyttäjien kokemaan luottamukseen. Työssä myös esitellään tekijät, jotka vaikuttavat positiivisesti käyttäjien kokemaan tietoturvaan ja sitä kautta parantavat käyttäjien luottamusta verkkopalveluun. Työssä osoitetaan myös, että tietovuodoilla on merkittävä negatiivinen vaikutus verkkopalvelun maineeseen, ja sitä kautta kuluttajien kokemaan luottamukseen. Työssä näytetään helppokäyttöisen käyttäjien tunnistustavan positiivinen vaikutus luottamukseen, sekä käyttökatkosten negatiivinen vaikutus luottamukseen.

Avainsanat:	luottamus, verkkopalvelut, digitaaliset palvelut, verkkoliiketoiminta, kuluttajakäyttäytyminen, yksityisyydensuoja, tietoturva
Kieli:	Englanti

Acknowledgements

I would like to thank professor Antti Ylä-Jääski for supervising this work, and providing feedback during the writing process.

I would also like to thank my employer Nixu, who sponsored the survey that is a central part of this work, and my former colleague Mikko Nurmi, who got me interested in this subject in the first place, and with whom I sparred the subject of online trust before doing this work.

Finally, I would like to thank Marjo. Without her love, support and understanding, I would not have been able to do this work during a time period that would have been the most hectic time of my life even without this work.

Helsinki November 20, 2017

Miska Laakkonen

Table of Contents

1. Introduction

1.1 Motivation

In most parts of the world Internet has become a platform where consumers carry out many of their daily routines and tasks such as shopping, communication with other people, getting the news or entertaining themselves. This creates a huge market for service providers who provide people with different types of online services such as online stores, social media services, dating services, news sites, or media streaming services. Lot of new players have emerged in this area, whereas many established companies have failed to compete with the new players even with three main advantages they have had over the newcomers: a brand that has already been known in the markets, trust relationship they may have been able to build with their existing customers, and the resources they have been able to gather during previous years in the business.

There is a consensus that a good end user experience is one of the key factors in regards to success of an online service. Therefore, service providers pay a lot of attention to end user experience when developing a new online service or upgrading an existing one, and service design companies have been successful in selling their expertise to service providers as experts on creating thriving online services. Cybersecurity companies on the other hand have not been that successful in offering their expertise in development of new online services. The goal of this study is to find out if the trust perceived by online service users towards an online service is a relevant factor in getting online service to succeed, and on the other hand what are those elements of trust that online service providers should focus on when developing a new online service, in order to get their online service to thrive.

1.2 Scope

This study examines the current research regarding the correlation between trust perceived by the online service users, their intention to purchase from an online service for the first time, and customer loyalty. This study also examines what are the elements that contribute to the trust experienced by the online service users. A model for studying how significant is the impact of different trust elements to the trust perceived by the online service user is presented. Based on the research model a survey is made for online service users. The significance of different elements of trust and their impact on trust, purchase intention and customer loyalty are analysed based on the survey results.

This study focuses on those trust elements that on one hand have a significant correlation with perceived trust, purchase intention and customer loyalty, and on the

other hand can be improved by enhancing cybersecurity of the online service. Therefore, some aspects of the trust building that are not related to cybersecurity are discussed in the literature review but not included in the research model and the survey.

1.3 Goals

Research problem for the study is to analyse which elements that contribute to the trust are seen relevant by online service users, and what is the impact of perceived trust to the success of an online service. Problem statement can be formulated as "From what elements the perceived trust towards online service consists of, and how critical are different elements for the success of an online service?"

The ultimate goal of this study is to find those trust elements that impact perceived online trust, and thus impact initial purchase intention and customer loyalty of online service user. The secondary goal is to compare the impact of different trust elements, and find out those trust elements that are most critical for the success of an online service.

1.4 Research Methods

The link between trust towards online service, initial purchase intention and customer loyalty is studied by examining existing research around this subject.

A trust model based on the existing research is created, and a research model for examining the cybersecurity-related elements that contribute to the trust perceived by the online service users is presented.

The significance of different elements in creation of trust towards online service is studied with a survey executed by TNS Gallup. A total of 779 respondents randomly selected from TNS Gallup's respondent base participated the survey.

1.5 Structure

This study consists of seven chapters and a short description of each chapter is provided below.

Chapter 2, Concept of Trust, describes the link between trust perceived by the online service users, the initial purchase intention and customer loyalty, based on existing literature.

Chapter 3, Research model, proposes a developed trust model, and describes the

research model used in this study.

Chapter 4, Survey, describes the survey that was done in order to find out what components contributed to the consumer customers' trust towards online services, and results of the survey.

Chapter 5, Analysis, analyses the results of the survey and highlights the key findings of the survey.

Chapter 6, Conclusions, reviews the findings of the study and summarizes how trust towards online service can be increased, and how this contributes to the success of the online service.

2. Concept of Trust

This chapter describes the importance of perceived trust towards an online service, and how perceived trust correlates with purchase intention and customer loyalty. This chapter also discusses what are the elements of trust according to existing studies, and different kind of online service trust models.

2.1 Online services and trust

Online service business has been growing rapidly during last decade, and the growth is expected to continue to the foreseeable future. Based on the reports released by U.S. Commerce Department, in 2016 e-commerce sales represented 11,7% of total retail sales, while 41,6% of the total retail sales growth came from e-commerce sales [1]. This indicates online business is becoming more relevant year-by-year, and as a result online service business has also gotten the attention of researchers.

As business is increasingly moving from brick and mortar stores to Internet, also the success factors for establishing a thriving marketplace are changing. Shopping has traditionally been a social activity, and consumers are typically influenced by their social interactions with others when making purchase decisions [2]. One notable factor hindering the growth of e-commerce is the decreased presence of human and social elements in the online environment [2]. Consumers will have to evaluate the trustworthiness of an online store based on other factors than direct face-to-face encounters with the representatives of the seller and other customers.

Potential success of an online service results as a combination of many different elements. Since there is no physical store the consumers are not able to notice the store on a visit on a trip to shopping mall, the consumers' awareness of existence of the online service plays a critical role. Usability of the online service, or perceived ease-of-use, is also important for the success of the online service. Traditional factors such as the competition that exists for the retailer or service provider, and the perceived usefulness of the goods or services offered for the customers are still relevant. However, among all the factors contributing to the success of an online service, trust experienced by the customer towards the online service has been identified as one of the key elements that define the success or failure of an online service [3][4].

While trust is a factor also in offline commerce, according to Yoon there are three main factors where online trust is different from offline trust: First of all, there is huge distance between the buyer and seller, secondly, the absence of sales person and thirdly there is no physical contact between the buyer and the product [5]. Trust with the online vendor is indispensable for reducing perceived risk [5]. Kim, Xu and Gupta suggest that unlike in traditional commerce, in the context of Internet shopping the perceived trust is

even more significant than perceived price [6].

Online service providers are typically aiming at two main goals: Getting as many visitors as possible while converting them into customers, and keeping them as repeat customers after the first interaction between the provider and the customer [7]. Initial trust towards the online service has been proven to be vital for purchase intention of a first-time customer, and repeat trust is vital for customer loyalty of an existing customer [7]. Initial online trust refers to the trust a customer with no prior interaction with the online service has toward service, whereas repeat trust refers to the trust formed toward online service based on prior experience [7].

In following chapters the connection between these two types of trust, and the resulting two items - initial purchase intention and customer loyalty - that are critical to the majority of commercial online service providers, are studied more in detail.

2.1.1 Trust and Purchase Intention

Purchase intention

In the context of this study, purchase intention refers to a situation where a consumer intends to become involved in an online transaction for the first time with a specific online service provider. Consumer may or may not be familiar with the service provider, and may or may not be familiar with the goods or services being purchased. While there are several factors that contribute to the purchase intention, initial online trust is one of the most relevant factors for consumers who are considering their first purchase with a new online service provider [4,5].

Perceived risk

By definition, risk is a necessary condition for trust to occur [8]. Perceived risk comes from an uncertainty encountered by the customers in the purchasing process due to possibility of bad purchasing decisions that might result from their subjective assessments in the decision-making process. Customers might face undesirable consequences due to bad decision. According to Kim et al., consumers' perceived risk can be defined as a consumer's belief about potential negative outcomes from the online transaction [9]. In the case of online trust and purchase intention, research shows that perceived risk negatively affects consumer intentions to transact with an online service [10]. On the other hand, according to research the perceived risk and online trust are positively related [11]. In other words, trust towards online service becomes more and more important when the risk related to potential purchase increases.

Trust and purchase intention

As discussed in the earlier chapter, the importance of trust in the online vendor stems from its role in helping consumers overcome perceptions of risk. For typical consumer web browsing feels safe, but making an online transaction is considered a huge risk [10]. High perceptions of online risk will adversely affect consumer willingness to share personal information, follow vendor advice, and, ultimately, purchase [10].

While trust towards the online service provider is a key element with all the customer segments, there are also differences between consumer types. One attribute of consumer that differentiates them regarding buying behaviour is the nationality of the consumer. For example, in China, consumers try to avoid uncertainty and risks when purchasing goods and services [3]. On the other hand, in the USA consumers do not have similar uncertainty-avoidance culture in their buying behaviour [3]. People with high uncertainty-avoidance culture try to evade conflicts and give high value on compromise [12]. Low uncertainty-avoidance cultures are associated with less regard for stability and permanence, and with greater risk taking [12]. Societies with high uncertainty-avoidance value durability, permanence, and solidarity, which can be considered as elements of online trust [12]. Uncertainty is reduced through the influence of other consumers, who share their personal experiences, or by observing peers using the online service [12]. Normative pressure from supervisors and peers to use the online service reduce uncertainty, since it suggests that using the online service is socially appropriate and perhaps even desirable [12].

Despite the differences between consumer types and nationality of the consumer, perceived risk and trust associated with the online service play a role in the purchase intention of the consumer. Even if the risk perceived by the consumer varies depending on consumer type, the same basic rule applies: when the risk perceived by the consumer becomes higher, also higher level of trust towards the online service is needed [3]. In other words, trust reduces the users' perceived risk and increases their intention to purchase from the online service [3,10].

Research shows there are multiple elements that influence consumers' purchase intention. Online service awareness as well as ease-of-use of the online service have a positive influence on purchase decision [2]. Also, consumer's familiarity with online transactions is positively related to purchase intention [4]. However, trust towards the online service has been pointed out as one of the most crucial factors influencing the purchase intention by numerous studies [2,3,4,5,7,9,10,11,13,14].

2.1.2 Trust and Customer Loyalty

Customer loyalty

In the context of this study, customer loyalty refers to a situation, where a customer purchases repeatedly from the same online service. When the online service tries to convert potential customer into a customer they try to get the potential customer to do an initial purchase decision, whereas in case of customer loyalty they try to convert customer into a repeat customer. Loyal customer is willing to buy more, spend more, is easier to reach, and acts as an advocate for the online service [15]. For these reasons, customer loyalty should be an objective at least for all commercial online services [15].

Trust and customer loyalty

Flavián and Guinalíu studied online service customer loyalty and came to a conclusion that consumers' loyalty to an online service is closely linked to the levels of trust [16]. The development of trust not only affects the consumers' purchase intention, but it also directly affects the effective purchasing behaviour, in terms of preference, cost and frequency of visits, and therefore, the level of profitability provided by each consumer [16]. Harris and Goode also studied the role of trust in customer loyalty of online service users, and came to a conclusion that trust plays a central role in online service dynamics and, in particular, in directly and indirectly driving customer loyalty [17]. Lauer and Deng came to similar conclusion, and state that greater customer trust results in greater customer loyalty [18].

Kim et al. studied the shared antecedents of trust between potential customers and repeat customers, and did not find any difference in strength of their effects on trust building [15]. However, they note that the results of their study should be interpreted with caution, because the test does not reflect the antecedents of repeat customer trust that result from experience gained from earlier transactions with the online service provider – service quality and customer satisfaction [15]. This suggests that while the trust is seen crucial for both purchase intention and customer loyalty, there might be additional elements of trust that contribute to the customer loyalty compared to the elements that contribute to the purchase intention [15]. To enhance and maintain repeat online trust, online service providers need to acknowledge that repeat customers do base their trust largely on their prior transaction experience with the same provider [7]. Therefore, attributes associated with the online service provider including its ability to deliver the product or service, its benevolence to customers, and its integrity in terms of its conduct can be emphasized during repeat online transactions [7]. Repeat customers, based on these positive experiences, are more likely to carry out another transaction with the same online service provider [7]. Initial trust weakens or strengthens by experience and trust building should be understood as a dynamic process [5].

As a conclusion, existing research indicates that trust is as vital to customer loyalty as it is to initial purchase intention. However, compared to the elements that contribute to the initial trust that affects the initial purchase intention, there are additional elements that contribute to the trust experienced by repeat customer, due to a fact that the customer already has got earlier experience with the online service.

2.2 Elements of Trust

2.2.1 Categorization

There is a vast amount of research studying components that contribute to the trust experienced by online service users. Some of the factors contributing to trust are similar in most studies, but there is also some variance between the studies and the factors proposed by them. Salo and Karjaluoto [3] proposed a model that separates trust influencing factors into external and internal factors, and this categorization is also used in this study, the main focus of the study being in internal factors.

External factors

External factors that contribute to the trust perceived by the online service user are factors over which online service providers have limited, or no control, and that are not directly related to the online service itself. Examples of such factors are product or service characteristics, consumer characteristics and individual preferences, differences between markets, cultures and countries and how those affect how risk related to online transactions is perceived [3].

Product or service characteristics seem to have a significant impact on how much people trust towards a service. Henriksen pointed out, that in Norway only 15% of people trust social media services, whereas 51% trust online services of private companies, 76% trust public services, and 85% trust police and healthcare systems [19]. Results might not be similar in some other countries, where trust towards government and public services such as police or healthcare services in general are not as high as in the Nordic countries. This emphasizes, that some of the external factors affecting the trust experienced by the user are actually a complex combination of multiple variables, which makes external factors hard to measure.

While the external factors influence perceived online trust, they mainly reflect individual preferences of online service users and are outside of the control of service provider. Therefore, they are not core focus of this study, and the theory and literature related to the external factors that contribute to the online trust are not discussed further.

Internal factors

Internal factors refer to trust building factors that are directly related to the specific online service and online service provider. Online service provider is able to influence these factors and thus improve - or reduce - the trust perceived by its customers. Internal factors differentiate online service from its competitors. Majority of the previous research also seem to focus on internal factors.

Privacy and security have been detected as major factors impacting online trust in almost all the literature related to consumer trust. Some researchers, such as Hoffman et al., propose that privacy issues, and lack of trust for security are the two most important reasons why consumers decline to purchase online [21]. Ganguly and Dash came to a similar conclusion in their study that found that Indian consumers consider privacy and security the most important factors in generating trust [13]. However, also partly contradicting interpretations exist - while Bart et al. also enlists privacy and security as drivers of trust experienced by online service users, they came to conclusion that brand image of the online service and service provider, and navigation and presentation of the website take precedence over privacy and security as drivers of online trust [22]. However, they point out, that the precedence of trust factors is dependent on the type of online service [22]. Privacy is usually most important for consumers who are using online services that are typically associated with information risks, such as community or social media services, and travel sites, whereas security is typically considered most important by consumers using online services that are typically associated with financial risk, such as financial services [22].

Kim et al. proposes that in the case of potential customers, reputation [based on second-hand information], and information quality [based on partial experience with the online service] have a significant relationship with trust [15]. In the case of repeat customers, in addition to reputation and information quality also perceived service level and customer satisfaction [based on overall evaluation of a customer's experience with the vendor] contributes to the online trust [15]. While reputation and information quality apply to both potential customers and repeat customers, service level and customer satisfaction apply only to repeat customers [15].

Koufaris and Hampton-Sosa concluded that trust perceived by new customers were affected by four main factors: Reputation, willingness to customize, ease-of-use and security [23]. Chen and Barnes proposed an extended trust model with nine elements: Usefulness, ease-of-use, enjoyment of technology, security, privacy, company size, reputation, willingness to customise and interaction between customers [4].

In this study, the internal factors contributing to trust are divided into following five categories:

category	*description*
Privacy	Perceived privacy and information protection provided by online service
Security	Perceived online service security
Reputation	Reputation and brand image of the online service and service provider
Usability	Usability, ease-of-use, navigation and web site quality of the online service
Other factors	Factors not directly related to online service but related to service provider, such as customer service quality, customer satisfaction

Table 1: The proposed categorization of internal factors contributing to trust

2.2.2 Privacy

Privacy refers to the protection of individually identifiable information on the Internet, and it involves the adoption and implementation of a privacy policy, notice, disclosure, and consent of the Web site visitors [22]. As previous chapter discuss, existing literature suggest the privacy is one of the main factors contributing to online trust, and on the other hand lack of trust is the main reason consumers are not willing to give their personal information to online services. Hoffman et al. pointed out in their study that consumers simply do not trust most online service providers enough to engage in exchanges that involve money and personal information with them, and that privacy issues are the main reasons behind this [21]. The lack of trust towards online service providers arises from the fact that consumers feel they lack control over the access that service providers have to their personal information during the online navigation process [21]. Nearly 63% of consumers who decline to provide personal information to online services report it is because they do not trust those who are collecting the data [21].

While privacy is a key driver of online trust, its influence on trust differs depending on type of the online service [22]. When consumers are making an assessment on whether a travel or community online service is trustworthy, consumers are more likely to consider privacy aspects than when they are visiting for example a computer site [22]. This is because a travel purchase will probably require more personal information about whereabouts and activities of a person than a computer purchase would [22]. Bart et al. concluded in their study, that certain type of online services such as travel or community services are associated with higher information risk than other types of services, and therefore privacy has also an emphasized relevance as a factor of perceived online trust [22]. Nevertheless, a correlation between privacy and trust towards online service was detected with all types of online services [22].

While there seems to be lack of trust by consumers towards online service providers,

there are privacy-related practices that service providers can engage in order to increase trust. Henriksen suggest, that in order to build an online service that is trusted by customers, the service provider should be clear and open and provide control of sharing their information to the users [19]. He lists transparency and control as two of the five key principles that enable trust towards an online service [19].

Transparency

In the context of online services and privacy, transparency refers to openness in how the personal information collected by the online service is going to be used. Transparency has become a relevant issue in modern Internet, since online services such as search engines and online retail stores are able to collect lot of data regarding consumers' behaviour on Internet. Distrust towards privacy practices of online services are a major issue for service providers, and according to Hoffman et al. 69% of online service users are not willing to give their information to online services if there was no mention on the site as to how the data would be used [21]. Hwang et Lee advise service providers to reduce uncertainty by formal rules of conduct [12].

Main tool for providing transparency and reducing uncertainty by formal rules of conduct is coming up with a public privacy policy. Lauer and Deng concluded that a stronger privacy policy leads to higher perceived trustworthiness, and on the other hand higher perceived trustworthiness leads to greater trust towards an online service [18]. Findings of Pan and Zinkhan support this view, and they propose that an online service with a clearly stated privacy policy communicates a "you can trust us" signal to visitors [24]. However according to them, while an online store that fails to include a privacy policy will lose consumers' trust, the contents of the privacy policy do not seem to have similar importance [24]. The wording of the privacy policy does not appear to have significant influence on consumers' perceived trust [24]. The reason behind this is that users do not typically read the policy [24]. They do not want to spend a lot of time on reading a lengthy policy description, often filled with legal jargon [24].

Pan and Zinkhan go on to suggest that the effect of public privacy policy might not be that significant among all consumer groups, since some are found to believe that by posting a privacy statement, organizations seek to escape liability or limit responsibility [24]. Therefore, though privacy statement signal a positive message, they do not free online service users from safety concerns [24]. Proposed solution to this dilemma by Pan and Zinkham is, that service providers should consider more effective approaches for safeguarding online privacy, as service provider's credibility can be enhanced by some easy-to-implement techniques [24]. They showcase simple examples that include secure icons that pop up at the bottom of the browser, and confirmation e-mails or pop-up windows that inform consumers about a transaction's status [24]. These small and simple acts can suggest to the consumer that the service provider operates a secure service [24]. However, these type of icons and pop ups are typically used to enhance perceived security by the online service users by for example signalling that transaction

is done in a protected manner, and are not often associated with privacy and transparency.

As a conclusion, past studies reveal that privacy is a major concern among consumers, and privacy-related risk reduces consumer trust in a particular online service [24]. Although some consumers have already accepted the risks embedded in online service use, privacy concerns may prevent many others from visiting the service [24]. As service providers increase their understanding of these factors and situations that foster privacy concerns, this knowledge can be employed to reduce consumer concerns and enhance consumer trust [24].

Based on these findings, following hypotheses are formed:

HYPOTHESIS 1: Clear privacy statement / terms of use increases perceived trust towards online service.

HYPOTHESIS 2: User is more likely to share his or her personal information with online service, if the purpose for which information will be used is communicated to the user in a clear and open manner.

Control

In the context of online services and privacy, control refers to a situation where user is given a control over what kind of personal information is stored in the online service, and which parties are able to access it, and to which purpose this information is used. Outside checking or unchecking a marketing permission on an online service, typically very few options to control personal information is given to the user.

Technically it would be relatively easy to give consumers the control over their personal information, but for some reason this has not been actively done. The reason could be, that online service providers fear that consumers would eventually deny any use of the information from providers.

Aimeur et al. found out that changing privacy policies with the purpose to allow users to understand the information stored of them, to manage the access to each element of their information and to earn from the use of this information, increases users' trust towards online service [25]. According to the study, it appears that current privacy policies lack profit for users, management of data, comprehension and private data control, which in fact are the key points for a privacy policy [25]. They suggest that online services should give users more control over their data and provide more flexibility in their privacy policies, and this would free the users from the dilemma of having to choose between two unappealing choices [25].

Based on these findings, following hypotheses are formed:

HYPOTHESIS 3: Control over personal information increases perceived trust towards online service.

HYPOTHESIS 4: Increased trust towards online service increases the likelihood that a user is willing to share personal information with online service.

HYPOTHESIS 5: Easy method for sharing personal information increases the likelihood that a user is willing to share personal information with online service.

HYPOTHESIS 6: User is more likely to share personal information with online service, if there is a profit for the user.

2.2.3 Security

Security of an online service refers safety of the computer and credit card or financial information [22]. It is considered as one of the main factors that affect customer trust in online commerce [22]. According to Global e-commerce report by Taylor Nelson Sofres Interactive [26] the following two reasons, which both are related to security, are the most important reasons why consumers do not purchase online:

- Don't want to give credit card details/security problems
- It's more secure buying goods and/or services in a store

However, according to Bart et al. the relationship between security and perceived trust c is different for different online service categories [22]. Security-related trust is typically considered most important by consumers using online services that are associated with financial risk [22]. Some online service categories, such as transaction oriented financial services, computer and travel sites, and online stores in general entail greater financial risk than some other categories [22]. When consumers purchase from online services that have products or services that are high-involvement items, they are more concerned about the exposure of financial information than with some other type of services [22]. For such online services, the impact of security on online trust is greater than it is for other online services [22].

Transaction security

In the context of this study, transaction security is used as a reference to the safety of online purchasing process. Since main inhibitors for consumers to buy online are the reluctance to give credit card details to an online service and greater trust towards

purchasing from traditional brick-and-mortar stores, it is easy to come to a conclusion that transaction security plays vital role in increasing consumer trust. Yoon has confirmed this in his study, where he found a correlation between transaction security and online trust [5].

Kim et al. suggested a model where technical protections and transaction procedures along with security statements are three contributors to the trust experienced by the user [27]. While in this study security statements are studied more in detail in chapter Security certificates, in the context of this study technical protections and transaction procedures are part in transaction security. Assumedly one of the most comprehensive technical protection methods of transaction security is that the data transferred over the Internet is securely protected. However, how that impacts the trust of the online service users in practise is unclear, especially due to a fact that many of the online service users might not be able to recognize whether the data actually is protected or not, and that makes it an interesting subject to study. Let's make an initial assumption that online service users of modern age are aware of whether the data is protected or not, and consider secure data transfer important, thus forming a following hypothesis:

HYPOTHESIS 7: Encrypted transactions increase perceived trust towards online service.

Reluctance to give credit card details is the main reason consumers decide not to purchase online [26]. Despite that payment providers such as Paypal have had considerable success and significant annual turnover growth [28]. This leads to another interesting hypothesis:

HYPOTHESIS 8: Using a well-known payment provider for transactions increases perceived trust towards online service.

Authentication level

During the existence of Internet, lot of authentication methods have emerged in addition to traditional mechanism where user authenticates to the online service using service-specific username and password combination. Online service providers have many different ways to implement strong authentication and social media authentication to their online service. Usage of strong authentication has been increasing on financial services and services provided by government, while social media authentication is often supported by community and streaming sites. Also, some online retail stores allow customers to link their social media identity with their user account.

However, still today most online stores use other than strong authentication methods to identify the customer. It is very common that online store customers are able to make purchases by just providing their credit card information, without any additional

authentication. As long as this is the reality, it is understandable that people are reluctant to purchase because they do not trust online service providers with their credit card information, as pointed out in the earlier chapters.

While there are studies that point out the importance of authentication as one of the key technologies to ensure security of the Internet, such as the study by Zhang et al. [29], there is limited amount of research regarding the impact of authentication to online trust. Kim et al. lists authentication as one of the transaction procedures in his study, but did not find significant correlation between transaction procedures and online trust [27]. However, the questionnaire used by their study did not include any mention of strong authentication. Since identification of the user should be considered as an integral part of online security, it is a valid assumption that by utilizing stronger, more advanced authentication methods, such as bank authentication, mobile phone authentication or biometric authentication, the online services would be able to increase the trust perceived by the users, compared to traditional, weaker authentication methods such as username-password authentication. This leads to another hypothesis:

HYPOTHESIS 9: Using strong authentication for user identification increases perceived trust towards online service.

Security certifications

Security certification refers to a security certificate that is shown for the online service users with a purpose of assuring them that proper measures are taken to achieve technical security. Typically, the security certificate is granted to the online service by an external party. Effectiveness of security certificates have been demonstrated by existing research.

Hu et al. concluded in their study that trust-promoting certificate, or seal, displayed for the users of an online store significantly influenced their trust towards online vendor, and their willingness to purchase [30]. Findings of Yoon [5] and Hwang and Lee [12] supported this conclusion. Also, Bart et al. suggest that security certificates, such as Better Business Bureau, Verisign, and TRUSTe, are considered to indicate required levels security by consumers, and therefore have a positive effect on perceived trust [22]. However, the security certificates alone do not themselves guarantee a trustworthiness of an online service. As Edelman points out, online services that have received security certificates might still have questionable behaviour regarding privacy issues, and a site that has received for example TRUSTe certification could still send hundreds of emails per week to its registrants [31].

Also, Hu et al. found out that although all the certificates included in the study influenced online trust, there was some variance between different certificates [30]. This could be related to how familiar consumers are with a specific certificate or certificate

issuer, thus leading to a situation where different certificates might impact online trust differently depending on the familiarity with the certificate or issuer on different markets and by different type of customer bases. Two hypotheses are formed based on these arguments:

HYPOTHESIS 10: Security certificate increases perceived trust towards online service.

HYPOTHESIS 11: The amount that security certificate influences perceived trust depends on user's familiarity with the certificate issuer.

2.2.4 Reputation

Reputation, in the context of the study, refers to perceived brand image and reputation of an online service provider. In the study focusing on initial trust building by McKnight et al. suggested that reputation is an important trust building factor particularly in the initial trust phase [10]. However, Kim et al. who compared trust building factors between potential customers and repeat customers found that reputation has significant impact on perceived trust towards online service provider both by potential customers and repeat customer [15]. Also Yoon came to a similar conclusion [5].

The perceived reputation of an online service is influenced by numerous factors: Online as well as offline marketing efforts, offline presence such as online retailers brick-and-mortar stores, second-hand information received from friends, word-of-mouth services such as website rating services, and potential past experience regarding the service provider can have an impact on reputation and perceived trust as well.

Lu et al. suggested in their study, that one important criteria in perceived trust towards an online service was whether the site had an offline presence or not [2]. One factor considered to influence reputation and thus, perceived trust among consumers, are so-called online WOM [word-of-mouth] services where consumers are able to rate online service providers, purchased goods and services based on their own experiences [20]. The impact of WOM to online trust appears to be gender-specific, and previous studies have come up with mixed results regarding their effectiveness [20]. Nevertheless, neither offline presence or WOM services are directly related to the online service itself, nor are they security-related factors. Therefore, these and other reputation influencing factors that are not in any way related to online service security, are outside of the scope of this study, and will not be further discussed.

However, there are also security-related issues that can have a significant impact on consumer trust. While high security level is often not visible to the consumer, the lack of proper security practises can potentially lead to severe damage for service provider's reputation. There are examples of companies that have suffered meaningful reputational

damage due to the data breaches, such as U.S based companies ChoicePoint and TJX [32]. It is reasonable to assume that data breaches in general, at least when they become public, have a negative impact on online service customers. This leads to following hypothesis:

HYPOTHESIS 12: Data breach disclosures have a negative impact on perceived trust towards online service**.**

2.2.5 Usability

Usability refers to availability, navigation, ease-of-use, and general quality of the online service. While quality, ease-of-use and overall user experience provided for an online service user are known to be independent factors that have a significant impact to the success of online services, existing research points out that usability also contributes to the trust perceived by the users towards the service. Choon Ling et al. concludes in their study that there is a positive relationship between perceived ease-of-use and usefulness and online trust [11]. Chen and Barnes did not find link between ease-of-use and online trust, but found a correlation between usefulness and online trust [4]. They also suggested that willingness to customize, which includes perception that online service responds to user's individual needs and thus can be considered as part of online service usability, also correlates with online trust [4]. Bart et al. found navigation and presentation of the website as trust building factors [22]. Therefore, there seems to be sufficient evidence that usability does have an impact on online trust and should be considered in this study.

Website quality

In the context of usability, website quality refers to general look-and-feel, navigation, presentation and features of the website. Everard and Galletta studied how perceived flaws affect perceived website quality, and found out that perceived website quality also influences the user's trust towards online service [33]. Flaws decreased perceived website quality, and decreased perceived website quality had a negative impact on trust [33]. Similar findings have been later reported by Gregg and Walczak, who studied impact of website quality to trust in context of online action vendors [34]. However, while website quality is acknowledged as a factor that influences online trust, in this context it should not be considered as a security-related factor of online trust. Focus of this study being security-related elements of online trust, website quality is not further discussed in this study, and is not included in the research model.

Authentication

In the context of usability, authentication refers to perceived ease-of-use of authentication methods provided by online service, rather that security-related aspects of authentication, such as strength of the authentication. While general ease-of-use of an online service is acknowledged as trust building factor by several studies, there is limited amount of research available regarding individual factors that contribute to the ease-of-use. Since authentication is in many cases the first procedure taken by a user who arrives to an online service, it is justifiable to study the impact of easy authentication to online trust, initial assumption being that easy-to-use authentication will have a positive impact on online trust. Thus, a following hypothesis is formed:

HYPOTHESIS 13: Easy-to-use authentication method increases perceived trust towards online service.

Availability

In the context of usability, availability refers to whether a website can be accessed at any given time. General assumption of online service users is that website can be accessed whenever needed. When there are no problems with online service availability, the high availability-level of the service tends to go unnoticed. However, customers usually leave quickly if website is not available when they try to access it [35]. Dickinger and Stangl found that availability of the website influences customer satisfaction and loyalty, even though they also point out that availability is not as significant factor regarding customer behaviour as some other factors such as ease-of-use of the website [36]. Since research suggests that decreased availability does influence customers, following hypothesis is formed:

HYPOTHESIS 14: Decreased availability decreases perceived trust towards online service.

Other factors related to usability

There are multiple other factors, that contribute to the online service usability, such as user's familiarity with online services, expectations based on earlier experiences and other personal variables such nationality and cultural background of the user [3, 5]. However, these are external factors discussed in chapter 2.2.1 and online service provider has a limited influence on these factors. Therefore, they are out of the scope of this study and will not be discussed further.

2.2.6 Other factors

There are also other factors that contribute to the trust, mainly in the case of repeat customers. Service quality, defined as capability of online service provider to provide goods or service reliably, and capability to respond to customers' needs promptly and accurately, has been pointed out as a major contributor to repeat trust [15]. Empathy on the other hand, defined as capability of online service provider to understand and adapt to different customer needs, have not been found to have as significant influence to online trust [15]. Nevertheless, these factors are related to service provider but not the online service itself, and therefore are not in the scope of this study and will not be discussed further.

2.3 Trust models

Different studies related to online trust approaches the subject from various angles. Some of them focus on correlation between online trust and purchase intention or customer loyalty, whereas some of them focus more on elements of trust and do not consider their impact on the customership. Therefore, also various types of trust models have been presented in existing literature. In this chapter, we discuss three of them.

Trust model proposed by Chen and Barnes

Chen and Barnes studied the impact of trust to purchase intention of a consumer, and presented a trust model for initial online trust [4]. In their model, elements that contribute to the trust are divided in three categories: Technology, perceived risks, and company competency [4]. They suggest that in addition to the elements within those three categories, also disposition trust, defined as individual's tendency to trust the other party in business environment, influences initial online trust [4]. The eventual purchase intention is formed based on trust and familiarity with online transactions [4].

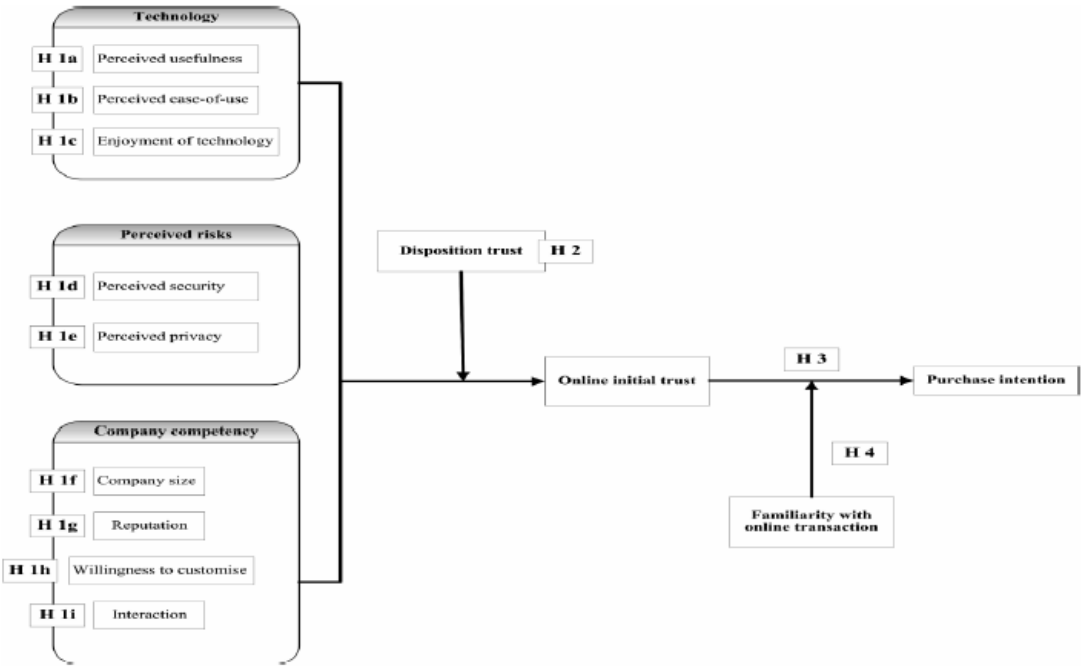

Figure 1: The conceptual model of online trust and purchase intention by Chen and Barnes [4]

As a conclusion of their study, they found correlation between technology, perceived risks, company competency and disposition trust, and initial online trust [4]. They also concluded that online trust and familiarity with online transactions influenced purchase intention as their model proposes [4]. However, no correlation between all the proposed elements and online trust were found [4]. Ease-of-use, enjoyment of technology, company size and interaction with consumers did not appear to influence initial online trust [4]. The fact that several elements within technology and company competency categories did not influence online trust, suggests that a different categorization might be more suitable for a trust model.

Trust model proposed by Ganduly et al.

Ganduly et al. proposed another trust model for online trust and its impact on purchase intention [13]. It is similar to the one proposed by Chen and Barnes [4], but lacks categorization of trust elements. On the other hand, privacy and security and separated from perceived risks, which is a logical evolution compared to model proposed Chen and Barnes [4], since risks such as monetary or information risks are a necessary condition for trust to occur, as defined by Mayer et al [8]. Trust model focuses entirely on internal factors, and external factors such as individual preferences and disposition

trust are omitted. Usability-related factors such as navigation design, information design and visual design are included to the model as individual elements, whereas privacy and security are not divided into individual sub-elements but are treated as a single entity. Dividing privacy and security into sub-elements would be a potential improvement to this trust model.

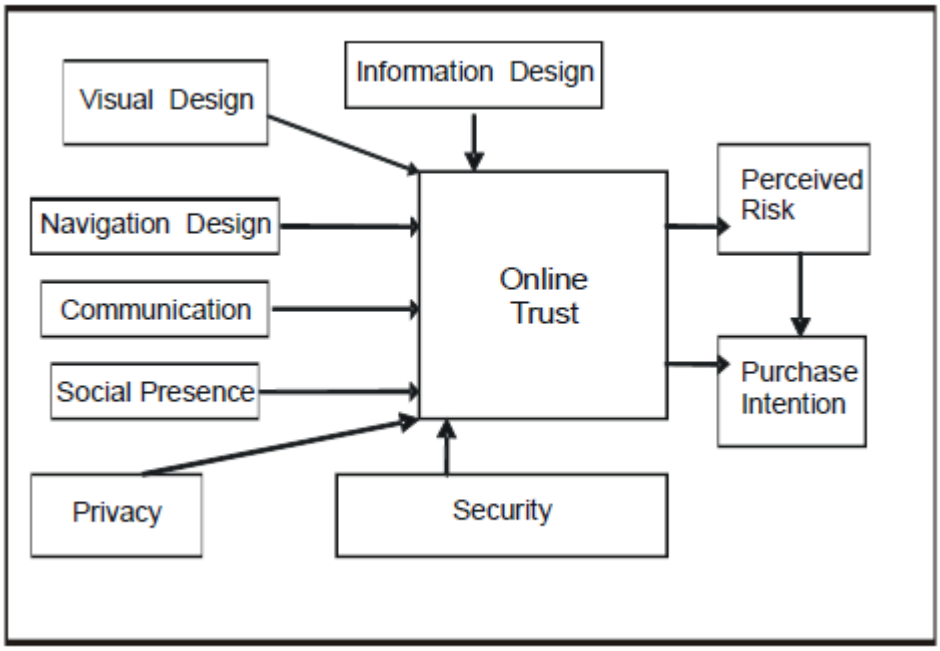

Figure 2: The trust model proposed by Ganduly et al. [13]

Trust model proposed by Salo and Karjaluoto

Trust model proposed by Salo and Karjaluoto [3] is the most comprehensive trust model presented in the reviewed research. Both external and internal factors contributing to online trust are considered in their model, as well as factors that contribute to repeat trust. Internal factors are divided into several subcategories, even though the categorization differs from the one used in this study.

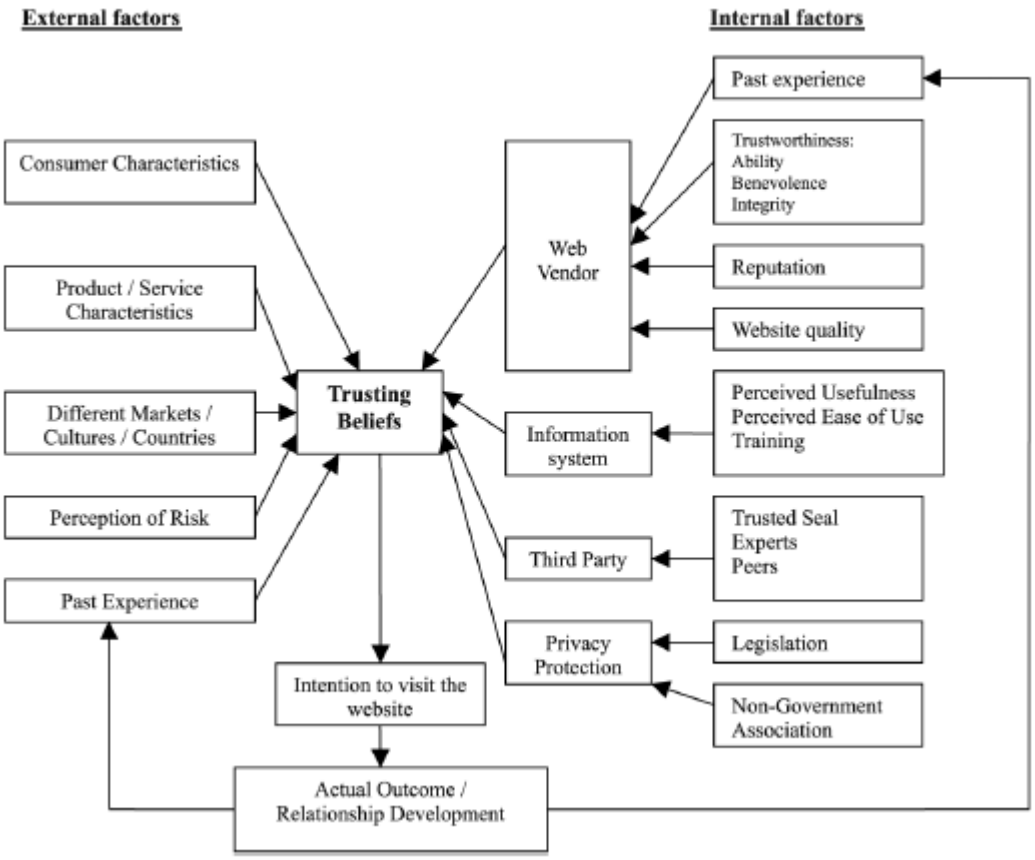

Figure 3: The trust model proposed by Salo and Karjaluoto [3]

Trust model of Salo and Karjaluoto extend beyond the scope of this study in certain aspects. The model includes external factors that are outside of the scope of this study as explained in the earlier chapters. Also, some internal factors such as legislation typically cannot be influenced by the online service provider and therefore are not considered in this study. Moreover, factors linked to trustworthiness of service provider – ability, benevolence and integrity – are not directly associated to the online service itself and therefore are excluded from this study. However, due to the comprehensiveness of the model, it acts as a good reference model for the research model used in this study.

3. Research model

Following chapters describe the developed trust model developed based on existing literature, and research model for the study.

3.1 Developed trust model

The trust model presented in Figure 4 was developed for the purpose of this study, i.e. for studying security-related elements of trust and their impact on perceived online trust, purchase intention and customer loyalty. The trust model is based on existing literature, and contains also elements that are not directly related to the online service itself. The highlighted items are the core elements regarding this study.

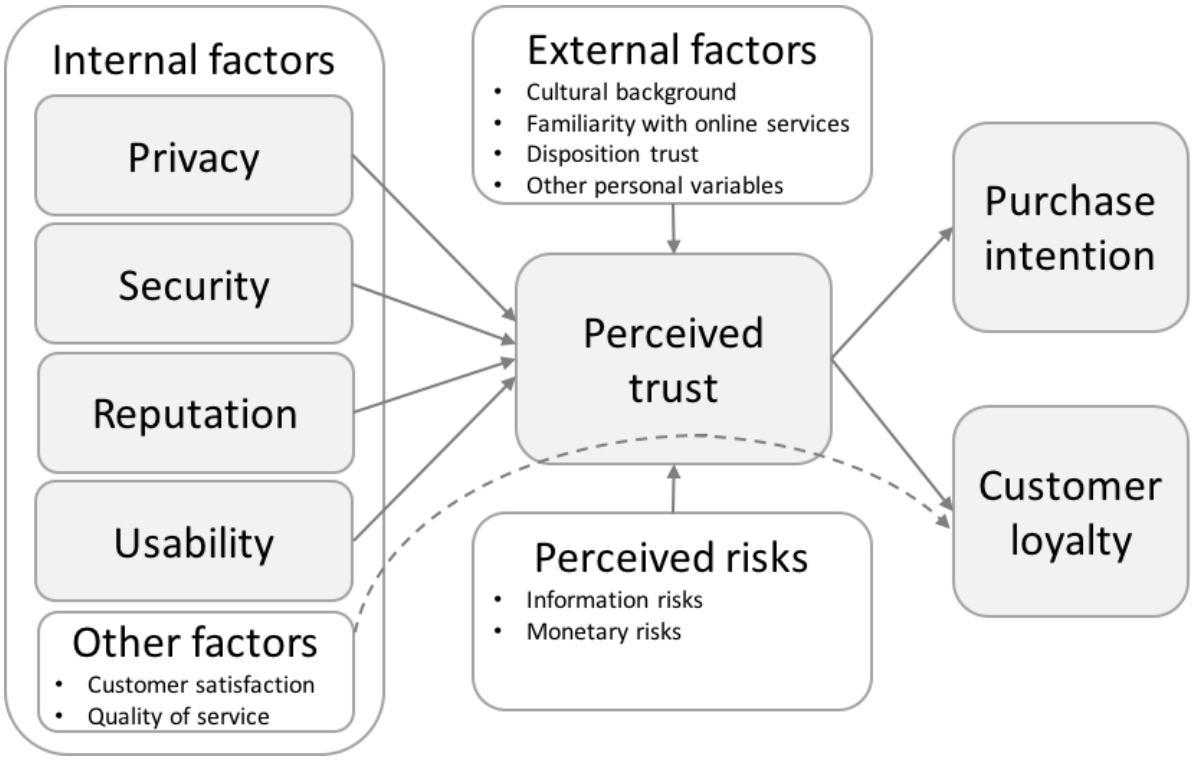

Figure 4: Trust model for studying security-related elements of online trust

External factors contributing to the perceived online trust are included in the model, and might have an impact on the online service development if the service is targeted for a

specific consumer group – for example people from different countries and cultures might have different expectations from online service privacy, or different age groups probably perceive usability differently. If the developed online service is targeted to a specific user group or groups, external factors should be considered when designing the online service security, and possibly there should be more emphasis on certain elements that contribute to the perceived trust. Differences between participant groups are discussed in the analysis section in those cases, where there are significant differences in how different participant groups perceive the influence of a specific trust element to online trust. However, external factors are not the core focus of this study.

Perceived risks are included in the model, but not considered in the survey, since the aim of this study is get an understanding on what are the elements that impact perceived online trust in a generic situation. However, perceived risk regarding the online service should be considered when the service is developed. If there is no information risk involved, probably there is no reason to focus on privacy of the online service, and on the other hand if there is monetary risk involved, the impact of security on perceived trust is probably different than in case of online bank.

Other factors, such as customer satisfaction and quality of service, are also included in the model, but not considered in the survey. These factors mainly contribute to the repeat trust and thus customer loyalty, but not initial trust required for purchase intention. Moreover, they are not related to online service security, but rather depend on service provider's customer processes – how they deliver the product or service, what kind of customer service they provide, etc. Therefore, they are outside the scope of this study. In the Figure 4, the relationship between these factors, perceived trust and customer loyalty is displayed with dashed line for better readability of the figure.

The core items of this study – Privacy, Security, Reputation, Usability, Perceived trust, Purchase Intention and Customer Loyalty – are discussed more in detail in following chapter.

3.2 Research model

Figure 5 describes the research model for this study. The core items from the developed trust model are included in the research model, and cybersecurity-related elements within each category of internal factors contributing to the perceived online trust (Privacy, Security, Reputation, Usability) are identified. Hypotheses (H1…H14) are also presented in the model, next to the potential trust influencing element they are related to. The categories, potential trust influencing elements and hypotheses related to them have been described in Chapter 2.

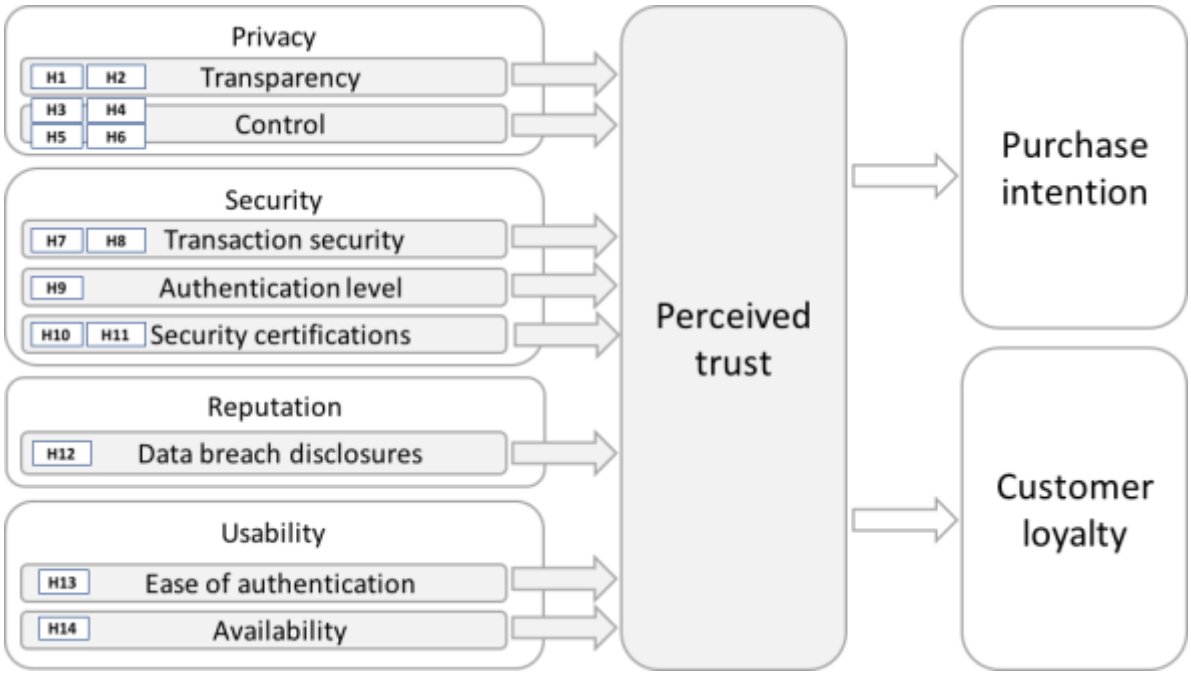

Figure 5: Research model for studying cybersecurity-related elements of trust

As discussed in chapter 2, existing literature provides strong evidence that perceived trust towards an online service has a significant influence on purchase intention and customer loyalty of online service users. Also, correlation between privacy, security, reputation and usability, and perceived online trust has been demonstrated by existing research. However, there is limited amount of research on cybersecurity related sub-elements of privacy, security, reputation and usability, and their correlation with perceived trust. This correlation will be examined by analysing results of the survey, and whether the hypotheses will be supported.

Privacy

Transparency refers to the openness of the service provider regarding their privacy practises. The goal of the study is to find out, how transparency influences perceived online trust (H1), and users' willingness to provide online service their personal information (H2).

Control refers to online service users' possibility to influence how the personal information they have shared with the online service will be utilized. The primary goal of this study is to find out, how control influences perceived online trust (H3), the secondary goal being to find out, what kind of actions could online service providers take in order to get users to share their personal information with the online service (H4,

H5, H6).

Security

Transaction security refers to security of monetary transactions. The goal of this study is to find out, how using encrypted transactions (H7) and external payment providers (H8) influences perceived online trust.

Authentication level refers to whether strong authentication or traditional username-password authentication is used. The goal of this study is to find out, how authentication level influences perceived online trust (H9).

Security certifications refer to security certificates given for the online service by external party, and displayed to the user visiting online service as a logo of certificate or certifier, possibly along with some more detailed description. The goal of this study is to find out, how security certificates influence perceived online trust (H10), and if there is a difference between influence on perceived online trust depending on whether the user is familiar with the party who has given the certificate (H11).

Reputation

Data breach disclosures refer to a situation, where an online service has been breached and data contained within the service has leaked to the intruder. The goal of this study is to find out, how data breach disclosure influences perceived online trust (H12).

Usability

Ease of authentication refers to how effortless it is for the users to authenticate themselves to the online service. The goal of this study is to find out, how ease of authentication influences perceived online trust (H13).

Availability refers to whether the online service can be accessed at any given time. The goal of this study is to find out, how interruptions in availability influence perceived online trust (H14).

4. Survey

This chapter describes the survey that was conducted for the purpose of studying how different elements of trust correlate with perceived online trust.

4.1 Background and demographics

The survey was conducted as an online questionnaire. TNS Gallup conducted the survey, and the respondents were selected among TNS Gallup's respondent base. All the respondents were between 15 and 69 years of age. Total of 779 respondents participated the survey.

Demographics of the survey respondents was following:

		%
Gender	Male	50
	Female	50
Age	15-24	17
	25-34	18
	35-44	15
	45-54	15
	55-64	13
	65+	22
Household type	Living with parents	9
	Single person household	31
	Adult household, no children	40
	Family with children	21
Occupation	Managerial employee	10
	Employee	30
	Student	15
	Retired	28
	Other	17
Area of residence	Helsinki capital district	21
	Other 50 000+ inhabitant city or suburb	38
	Other district	41

Household income	Less than 35.000 €	41
	35 – 50.000 €	21
	50 – 85.000 €	27
	More than 85.000 €	12
Online buying behaviour	Buys online all the time	3
	Buys online regularly	25
	Buys online occasionally	44
	Buys online seldom	17
	Has tried buying online	5
	Has never tried buying online	5
	Cannot say	1
Digital behaviour classification	First adopter	3
	Active	21
	Observer	45
	Passive	29
	Cannot say	3

Demographics of the respondents are personal variables, as described in the developed trust model. In case there are significant differences in responses given by respondents to a specific question, the differences and potential reasoning for those differences are analysed.

The results of the survey are weighted to match actual demographics of population of Finland regarding gender, age groups and area of residence.

4.2 Survey results

Appendix 1 summarizes the survey results. The summary of survey results contains responses of all 779 respondents categorized under different trust element categories as described in research model in chapter 3.2., and weighted to correspond with demographics of population of Finland.

In the summary of survey results, 95% confidence interval is shown next to the column that describes division of responses. Confidence interval describes the lower and upper limits for a specific response with 95% probability, if the survey was conducted for the whole population of Finland, and would include inhabitants who are between 15 and 69 years of age.

Cross-tabulated survey results are not included in the *Appendix 1: Summary of survey results*, but differences in answers of different demographic groups are discussed in chapter 5 whenever that is relevant.

5. Analysis

This chapter describes and analyses the results of the survey. Analysis and diagrams are mainly based on responses of all the 779 survey participants, but responses of different demographical respondent groups are briefly discussed in those cases when there are relevant differences between them. All hypotheses formed in chapter 2 are validated based on the findings and analysis.

5.1 Privacy

Existing literature suggests, that there is a correlation between privacy and online trust, as pointed out in chapter 2.2.2. This chapter examines, how different elements related to privacy on one hand correlate with perceived online trust, and on the other hand impact users' willingness to share personal information with the online service.

5.1.1 Transparency

In chapter 2.2.2, an assumption was made that a clear and easy-to-understand privacy statement / terms of use have a positive impact on perceived trust towards online service, and that openness regarding the purpose for which personal information will be used increases users' willingness to share information with the online service. This chapter discusses validity of these assumptions based on survey results.

Impact of clear and easy-to-understand privacy statement

Figure 6 describes how the respondents answered, when they were asked about impact of easy-to-understand privacy statement / terms of use on perceived trust.

86% of respondents found that clear and easy-to-understand privacy statement greatly or somewhat increases their trust towards the online service, while only 2% of respondents said clear and easy-to-understand privacy statement does not impact their trust towards online service at all. The responses leave little room for interpretation – assumption among consumers is clearly that the wording of privacy statement does have a significant impact on their trust towards online service.

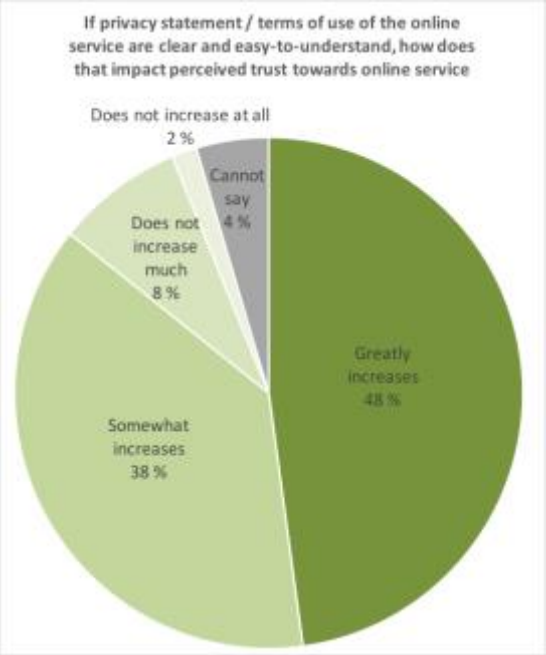

Figure 6

However, as pointed out in the Chapter 2.2.2, consumers might not read privacy statements or terms of use before approving them, because the general expectation is that privacy statements or terms of use are filled with legal jargon. While the survey results suggest almost all Finnish consumers believe that a clear and understandable privacy statement or terms of use have a positive influence on their online trust, there might be a difference between how consumers believe a clear privacy statement will impact their trust towards the online service, and how a clear privacy statement does impact their trust towards the online service in practise. Therefore, further study examining whether the consumers really notice a situation where the privacy statement is clear and understandable would be needed, since this is a pre-condition for the wording of privacy statement to impact online trust. Nevertheless, results of this study support the assumption that clear privacy statement or terms of use increase perceived trust.

Thus, *Hypothesis 1: Clear privacy statement / terms of use increases perceived trust towards online service* is supported.

Impact of openness regarding how personal information will be used

Figure 7 describes how the respondents answered, when they were asked about impact of openness regarding how personal information will be used to willingness to share information with the online service.

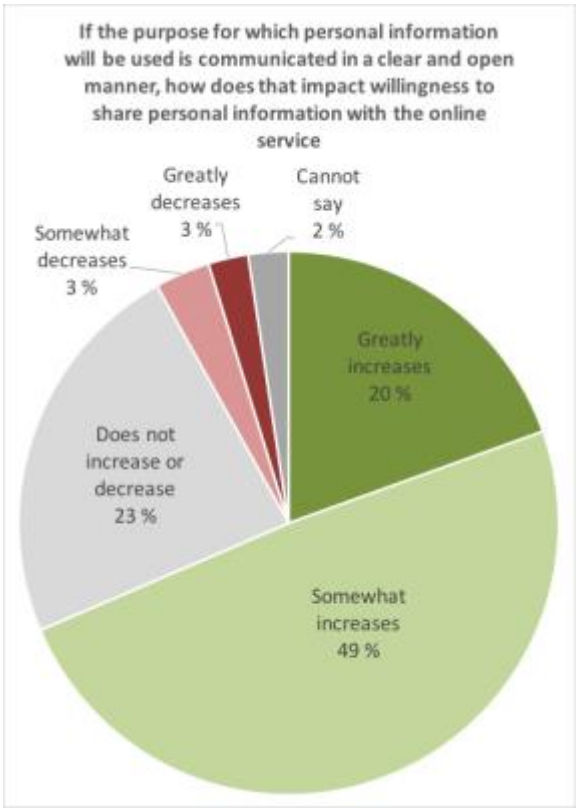

Figure 7

69% of respondents believe that they are more willing to share information with the online service when the service provider is open regarding the purposes for which the information will be used. 23% of respondents say there is no impact on willingness to share information with the service provider, and 6% of respondents believe the impact is negative. While the results clearly show positive correlation between openness and willingness to share information, the negative impact might occur when the personal information is used in a way that is not acceptable by some of the users. However, results suggest that service providers should indeed pay attention to openness regarding how they will use personal information given by their customers, if they want their customers to share personal information with them.

Thus, *Hypothesis 2: User is more likely to share his or her personal information with online service, if the purpose for which information will be used is communicated to the user in a clear and open manner* is supported.

5.1.2 Control

Impact of control over personal information

Figure 8 describes how respondents answered, when they were asked how does it affect their trust towards online service when they are given control over how the personal information they have shared with the service will be used.

The respondents say almost unanimously (92%) they trust the online service more if they are able to control usage of their personal information. Only 5% of the users think the control does not increase or decrease their trust towards the service, whereas 0% of respondents think there is a negative impact on trust. The obvious interpretation of the results is, that service providers would benefit in terms of perceived trust, if they allowed more control for their customers over the usage of their personal information.

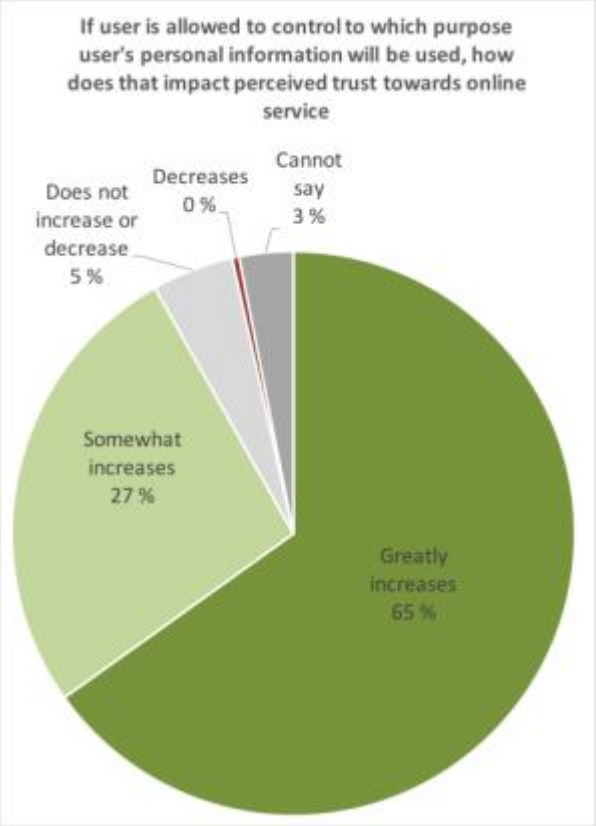

Figure 8

Also, another control-related question was presented for the survey participants. Figure 9 describes responses to a question whether possibility to modify or remove personal information gathered by the online service impacts users' trust towards the online service.

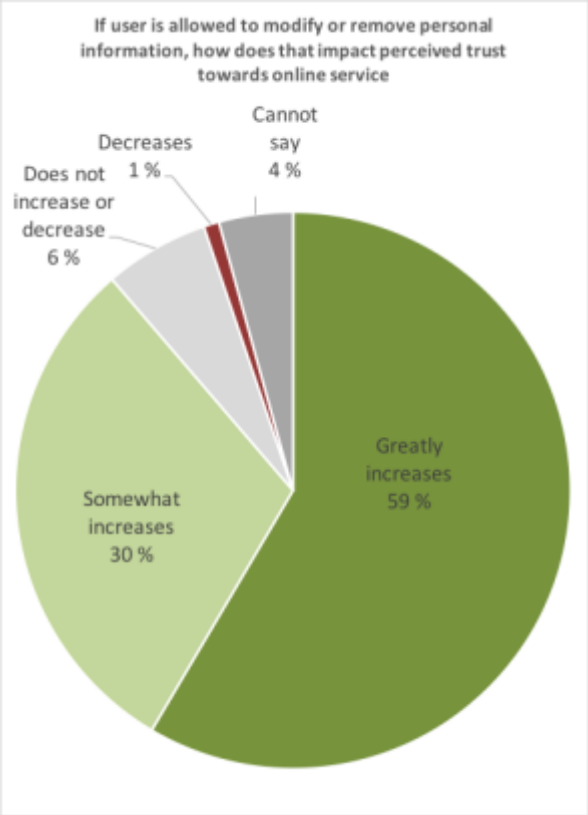

Figure 9

Results are very similar to previous question: 89% of respondents believe the control they are given over their personal information in form of possibility to modify or remove personal information either somewhat increases or greatly increases their trust towards to online service. Only 6% believe there is no impact, and 1% say it decreases their trust towards the service.

As a conclusion of these two control-related questions, vast majority of respondents say that control over their personal information increases their trust towards the service.

Thus, *Hypothesis 3: Control over personal information increases perceived trust towards online service* is supported.

Impact of trust on willingness to share personal information

Figure 10 describes whether the respondents agree with the statement that they are more willing to share personal information with the online service when their trust towards the service increases.

Almost half (47%) of the respondents either strongly agree or somewhat agree with the statement, whereas 29% disagree and 21% do not agree or disagree. It is noteworthy, that bigger percentage of respondents strongly disagree than strongly agree, while somewhat agree is the most common response given by the survey participants. While there is some evidence that trust increases willingness to share personal information, it is not as strong as with previous arguments. Therefore, it is relevant to also consider differences between different respondent groups.

Figure 11 describes the responses by active online buyers (N=198), and figure 12 describes the responses of respondents who have either only tried buying online or do not buy online at all (N=240). There are significant differences between these two respondent groups. 58% of active online buyers either strongly agree or somewhat agree with the statement, whereas only 33% of respondents who do not buy online strongly agree or somewhat agree with the statement. Correspondingly, only 20% of active buyers disagree with the statement, whereas 38% of respondents who do not buy online

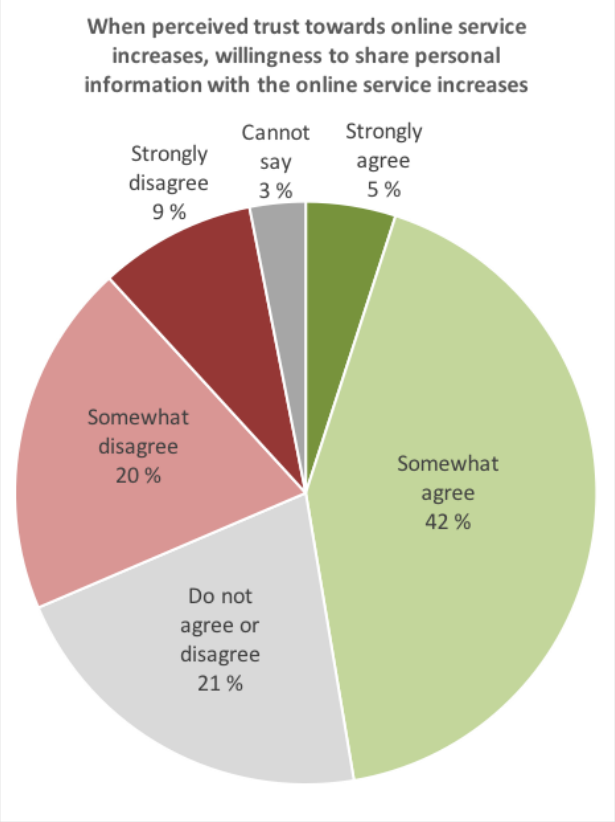

Figure 10

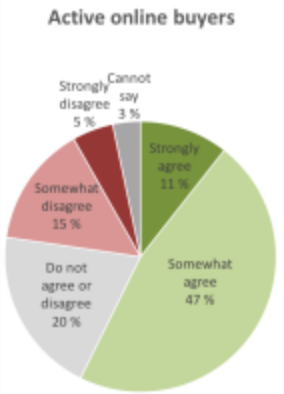

Figure 11

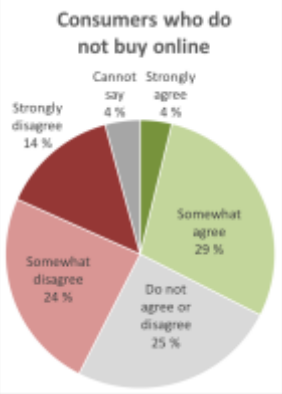

Figure 12

disagree.

There is a correlation between perceived online trust and willingness to share personal information with the online service, even though it is not as significant as in the case of some other survey questions. On the other hand, majority of active online buyers, which is the main target group for majority of commercial online services, agree with the statement. Considering these factors, the conclusion is that *Hypothesis 4: Increased trust towards online service increases the likelihood that a user is willing to share personal information with online service* is supported.

Impact of easy method for sharing personal information

Two different scenarios were included in the survey to examine how the easiness of sharing personal information impacts willingness to share personal information. In the first scenario, the user will have to share only small amount of information at time, i.e. user would not have to fill in large forms with lot of fields all at once. In the second scenario, the online service would fetch personal information from a social media service, such as Facebook, without users having to type the information themselves.

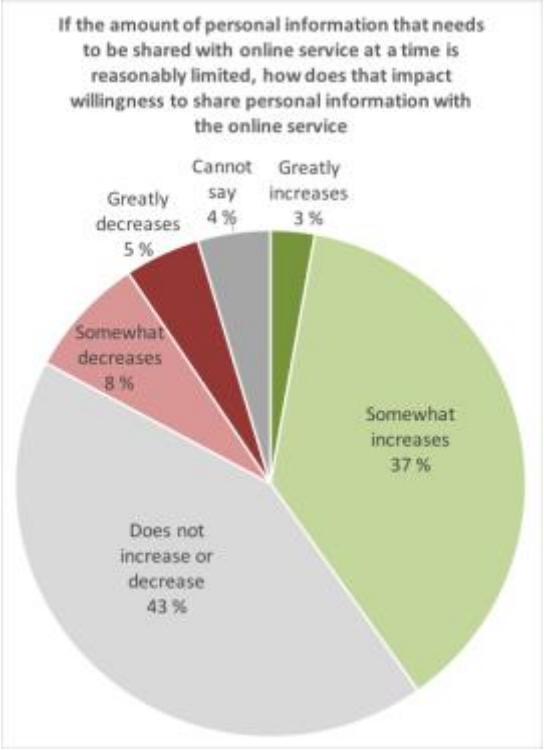

Figure 13

Figure 13 describes survey results regarding the first scenario. 3% of respondents indicate that possibility to share small amount of information at a time would greatly increase their willingness to share information with the online service, and 37% say the willingness to share information somewhat increases, whereas 43% of respondents conclude that there is no impact on their willingness to share information.

There are also differences between respondent groups: 52% of consumers who are active online buyers say that possibility to share small amount of personal information at a time either greatly increases or somewhat increases their willingness to share information, whereas among consumers who do not buy online the corresponding figure is 29%. The respondent group with most positive reaction to this scenario is women aged 15-24, with

59% saying this kind of method where personal information is given bit by bit increases their willingness to share information. Apparently, the survey results regarding the first scenario suggest that there is a positive correlation, even if not a particularly strong one, with easiness of sharing personal information and willingness to share personal information.

However, using a social media service as an easy personal information sharing method does not seem to have similar positive impact on willingness to share information with the online service – on the contrary, as seen in Figure 14, almost half of the respondents (49%) say that if the social media service fetches their information from a social media service it somewhat decreases or greatly decreases their willingness to share information with the online service. Only 14% of respondents think that this would greatly increase or somewhat increase their trust towards online service.

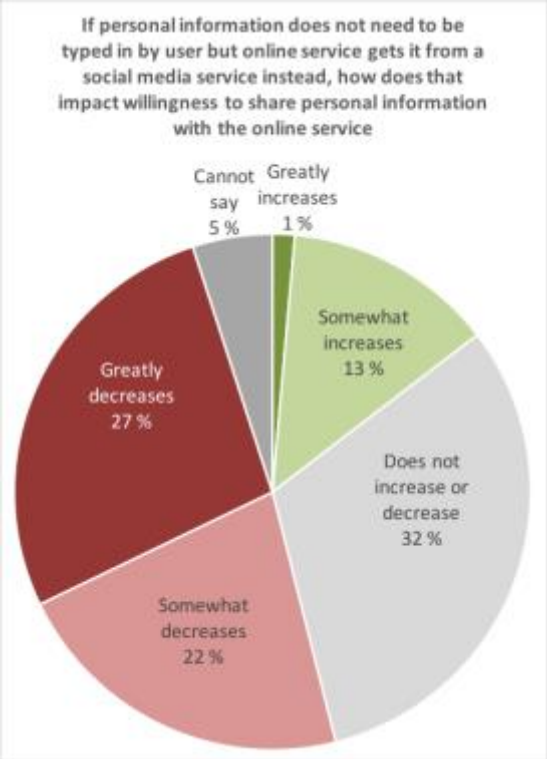

Figure 14

This is most likely caused by a general distrust towards social media services, since especially Facebook has gotten lot of negative attention due to privacy issues. Nevertheless, the result indicates that the increase or decrease in willingness to share information is dependent on the method that is used for easier information sharing.

Based on the findings, *Hypothesis 5: Easy method for sharing personal information increases the likelihood that a user is willing to share personal information with online service* is partially supported. While there evidently are ways to enable easier methods for sharing personal information and thereby increase users' willingness to share information, this does not apply to all the methods, such as fetching the information from a social media service.

Willingness to share personal information for a profit

The survey included two questions aimed to examine whether willingness to share information with the online service increases, if the user profits from sharing the information. In the first question, the profit offered for the user was a discount, and in the second question the profit was better end user experience.

Figure 15 describes division of responses when the survey participants were asked whether they agreed or disagreed with the statement saying benefit such as discount increases their willingness to share information. 33% of respondents agree with the statement.

There are also significant differences between different respondent groups: 48% of active online buyers agree that discount increases willingness to share personal information with the online service (Figure 16), whereas in case of respondents who do not buy online, only 23% of respondents report increased willingness to share information (Figure 17).

Women aged 15-34 are most likely to share personal information when given discount (58%), which is a worth noting, since many online retail stores are targeted for young women.

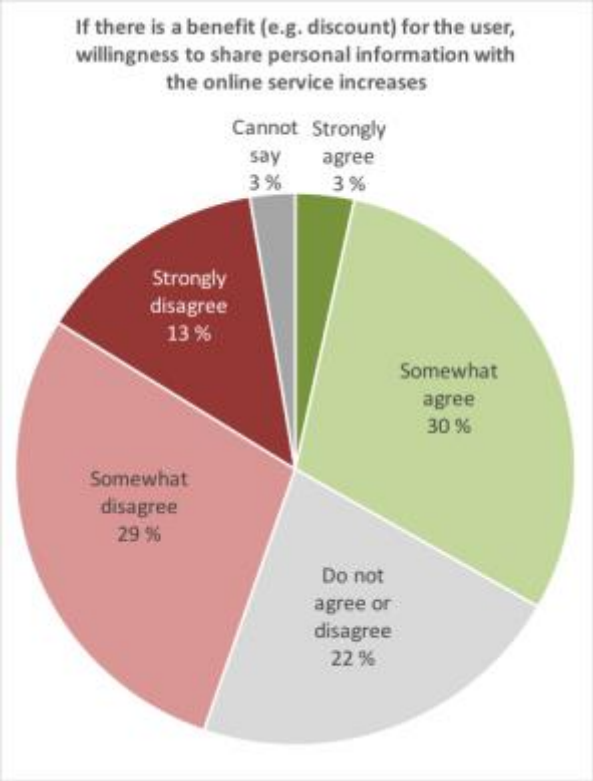

Figure 15

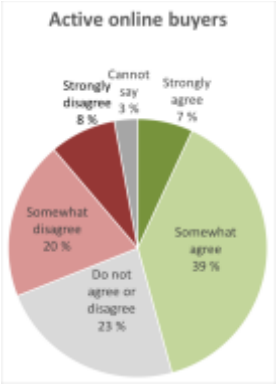

Figure 16

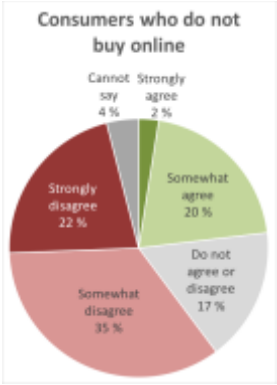

Figure 17

Figure 18 describes how willingness to share personal information with the online service is affected when it leads to better end user experience. End user experience can be improved for example by customizing the website and offerings based on individual preferences of the user. 39% of users agree with the statement, while 45% either do not agree or disagree, or cannot say whether there is an impact to willingness to share information. Only 16% disagree with the statement.

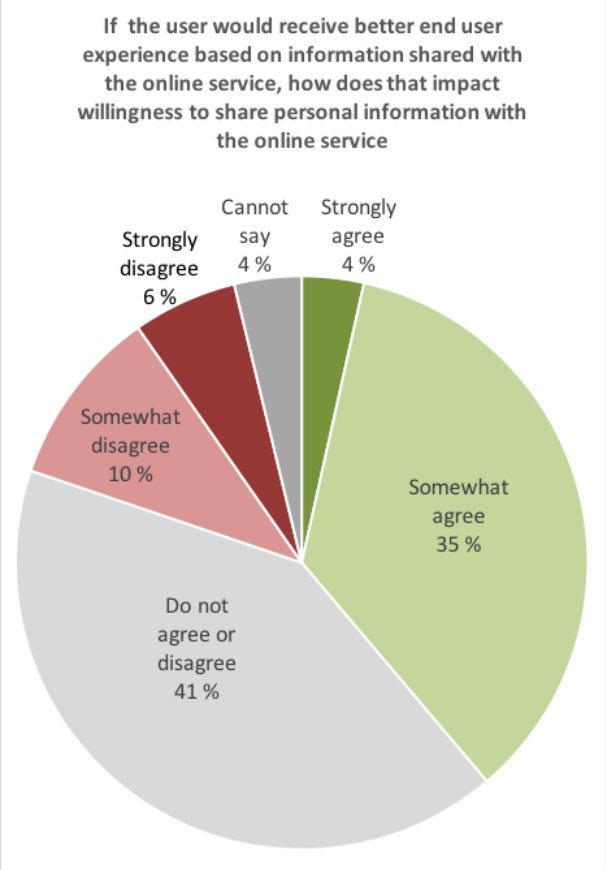

Figure 18

Also in this case, almost half (49%) of active buyers agree with the statement (Figure 19), while the number of respondents who agree with the statement is much lower among consumers who do not buy online, with only 28% agreeing with the statement (Figure 20). Also in this scenario, the women aged between 15-34 are most willing to share their personal information when it leads to improved end user experience, with 59% of them agreeing with the statement.

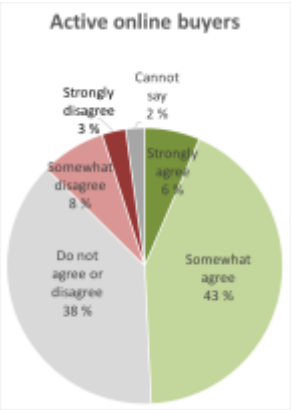

Figure 19

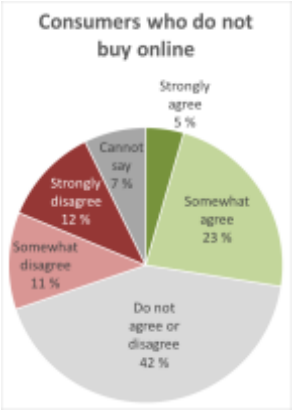

Figure 20

While majority of the users do not seem to be willing to share their personal information for improved end user experience, significant number of respondents say they are indeed more willing to provide information for the service to get better, more personalized user experience. Therefore, a clear positive correlation between better end user experience and willingness to share personal information can be found.

Based on these two scenarios where user gets some kind of profit for sharing their personal information, *Hypothesis 6: User is more likely to share personal information with online service, if there is a profit for the user* is supported.

5.2 Security

Existing literature suggests that there is a positive correlation between security and online trust, as pointed out in Chapter 2.2.3. In this chapter we examine, what individual elements of security impact perceived online trust.

5.2.1 Transaction security

Importance of encrypted transactions

Transaction security is described by existing literature as one of the main factors contributing to the online trust. Encrypted transactions are considered as one of the key elements in order to make transaction secure. When participants were asked how important they consider encrypted transactions in terms of transactions security, the results seem to support this notion, as seen in Figure 21.

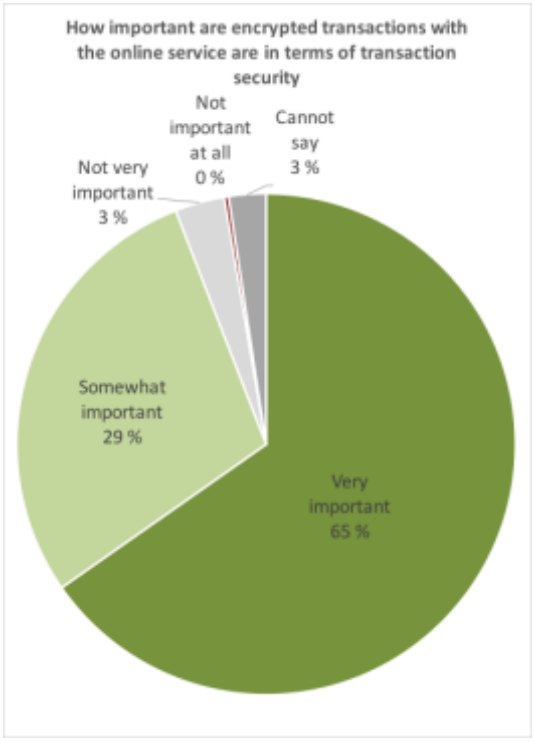

Figure 21

Almost all the respondents consider encrypted transactions important in terms of transaction security, with 94% of survey participants finding encrypted transaction either very important or somewhat important to transaction security, whereas only 3% find encrypted transactions not to be very important. This leaves little room for interpretation – encrypted transactions clearly impact perceived transaction security. However, in order for encrypted transactions to influence online trust, the users of an online service will also need to recognize a situation where transactions are encrypted.
To study this, the respondents were also asked if they recognize a situation where the transaction are encrypted, and the results are described in Figure 22.

73% of respondents say they do recognize a situation where transactions are encrypted. Since almost all the respondents believe transactions need to be encrypted, and majority of respondents also claim they recognize a situation when the transaction is encrypted, the conclusion is that *Hypothesis 7: Encrypted transactions increase perceived trust towards online service* is supported.

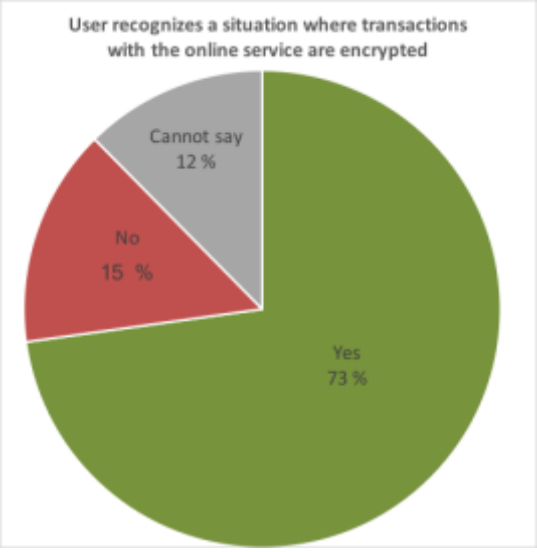

Figure 22

Impact of well-known payment provider on perceived online trust

It is somewhat common for online services to use external payment provider for online transactions. External payment provider can be an online bank, or other type of payment service provider such as Klarna or PayPal, that allow customers to make the payment either via online bank transfer or by sharing their credit card number with the payment provider. Instead of using external payment providers, many online services support only direct transactions between the customer and the online service. In this case the customer shares their credit card number with the online service, and the service provider then directly charges customer's credit card for the purchase. This study examines, how using external payment provider impacts perceived online trust compared to direct transactions with the online service.

As the results show, Finnish consumers consider online bank payment the most secure payment option, with 91% of respondents considering online bank payment either very secure or somewhat secure. Nordic payment providers and international payment providers are also considered significantly more secure than direct credit card transactions with the online service, with 55% and 48% respectively considering them secure. Only 22% of respondents consider direct credit card transactions with the online service to be secure.

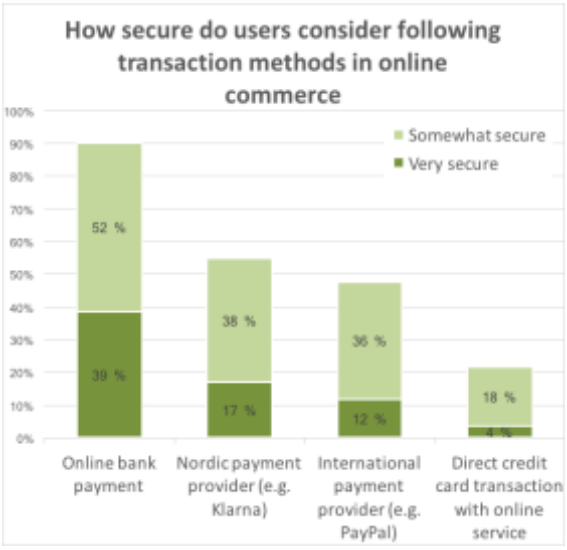

Figure 23

While the results clearly point out that external payment providers are considered to be significantly more secure than direct transactions, it is worth noting that there are also significant differences between external payment providers: Only roughly half of the number of respondents that consider bank payment secure do consider transactions via international payment provider secure. While the results to this particular question could differ significantly with respondent group that represent different nationality than the respondent base of this survey, the results should be considered at least by service providers who are targeting Finnish customers when they are making decisions about external payment providers they are going to use when developing a new online service.

Since the survey results indicates that external payment providers are considered more secure than direct transactions with the online service, and on the other the existing literature suggests that transaction security increases trust towards online service, *Hypothesis 8: Using a well-known payment provider for transactions increases perceived trust towards online service* is supported, with the notion that there are differences between external service providers in terms of perceived security.

5.2.2 Authentication level

Impact of authentication level on perceived online trust

The impact of authentication level on trust was studied by asking the respondents how it impact their trust towards online service, if they are identified with a specific authentication method. Three of the authentication methods included in the survey are considered as strong authentication methods: Bank-ID authentication, mobile phone

authentication and biometric authentication (biometric authentication refers to an authentication done for example based on facial recognition made using the camera of the mobile phone or laptop, and this example was also described for the respondents to clarify the meaning of biometric authentication). In this survey, traditional password authentication represented weak authentication method. Figure 24 describes the results for this survey question.

Bank-ID was considered as an authentication method that increases the trust towards online service the most, with 80% of respondents saying using Bank-ID for identification either greatly increases of somewhat increases their trust towards online service. However, the other strong authentication methods – mobile phone authentication and biometric authentication – are viewed as trust-increasing methods for identification only by 29% and 24% of respondents, respectively, whereas 53% of respondents are saying password authentication increases their trust towards online service.

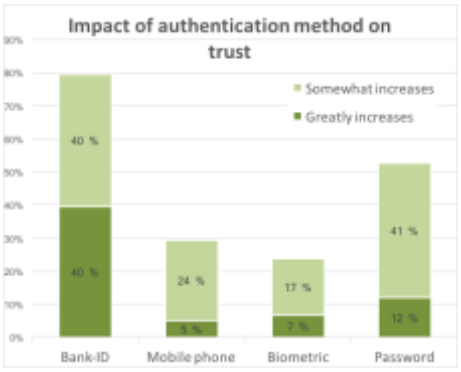

Figure 24

The results suggest that using strong authentication does not necessarily increase perceived trust towards online service when compared to weak authentication. One reason for higher perceived trust towards password authentication compared to stronger authentication methods could be that consumers are not yet familiar with strong authentication methods and how they will be used, since they are currently relatively uncommon, and most online services do not support that type of authentication at the moment. Once people get more accustomed to those authentication method, their impact on perceived trust might increase. However, currently the password authentication increases trust to online service more than strong authentication even among active online buyers, with 37% saying mobile phone authentication increases their trust towards online service, compared to 59% who say password authentication increases their trust.

Based on these results, *Hypothesis 9: Using strong authentication for user identification increases perceived trust towards online service* is not supported.

5.2.3 Security certificates

According to existing research, there are indications that security certificates influence perceived trust, but there is also some variance between different types of certificates, as pointed out in chapter 2.2.3. The goal of the survey was to verify the impact of security

certificate on perceived online trust, and to find out if users' familiarity with the certificate issuer does also have an impact on perceived online trust.

Impact of security certificates on perceived online trust

Figure 25 describes the results when the respondents were asked whether security certificate makes them more likely to trust an online service. 53% of respondents report increased trust towards a service that has a certificate that verifies it has passed a security audit, whereas 22% report their trust is not affected by security certificate, with 25% stating they are not able to say whether the certificate impacts their trust towards online service or not.

Since majority of the respondents consider security certificate to increase their trust towards the online service, *Hypothesis 10: Security certificate increases perceived trust towards online service* is supported.

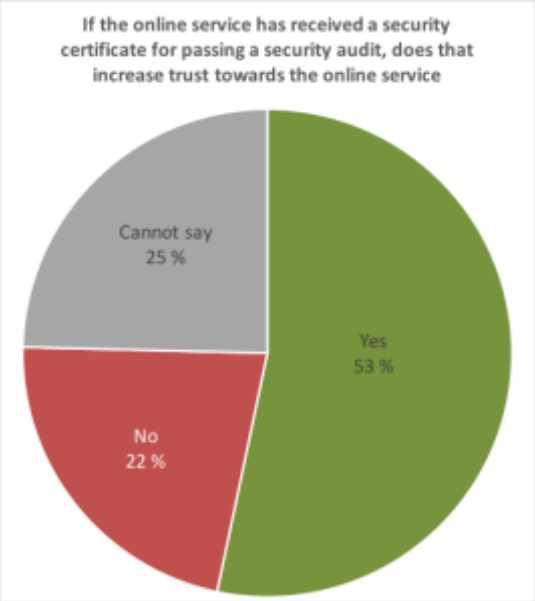

Figure 25

Impact of familiarity with the certificate issuer on perceived online trust

When respondents were asked in which case the certificate positively impacts trust towards online service, the results leave more room for interpretation. Most significant factor among Finnish consumers seems to be whether the certificate is issued by a Finnish company, with 37% of respondents saying certificates issued by a Finnish company increases their trust. 24% of respondents report increased trust when the certificate is issued by a company they know by name, whereas only 9% report increased trust in case the certificate is issued by a foreign company.

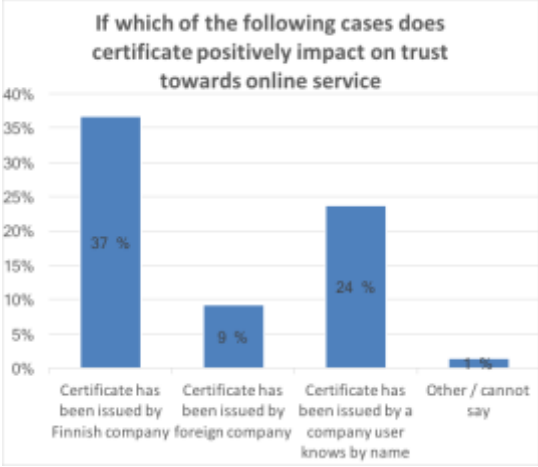

Figure 26

The interpretation of the results is not unambiguous. Certificates that are issued by a

Finnish company increase perceived trust towards online service significantly more among Finnish consumers, than a certificate issued by a foreign company. One interpretation of the result could be, that consumers trust towards the online service increases more in case of Finnish certificate issuer because Finnish consumers tend to trust domestic companies more than they trust foreign companies, possibly because they know that domestic companies need to operate under legislation of Finland which Finnish consumers are more familiar with. Whatever the reason, home country of the issuer seems to be more important than consumers' familiarity with the certificate issuer, while certificates issued by familiar company still increase trust more than certificates issued by foreign companies.

While the results are mixed, certificates issued by a company the consumer knows by name still seem to increase trust towards the online service than certificates issued by an unknown foreign company. A certificate issued by Finnish company increases trust more than a certificate issued by a company the consumer knows by name, but then again, the trust Finnish consumers experience towards certificates issued by Finnish companies can still be interpreted as sort of related to familiarity with the issuer. Based on the results, *Hypothesis 11: The amount that security certificate influences perceived trust depends on user's familiarity with the certificate issuer* can be considered partially supported. However more research is needed before conclusive statement regarding the hypothesis can be made. It is also worth noting, that implementing similar survey to a respondent base with a different nationality could result somewhat different conclusions.

5.3 Reputation

Existing literature shows that reputation is one of the key factors contributing to the online trust, as pointed out in chapter 2.2.4. In this chapter, the impact of data breaches on reputation, and thereby perceived online trust is discussed.

5.3.1 Data breach disclosures

Impact of data breach disclosures on perceived online trust

Figure 27 describes the impact of data breach disclosure on perceived online trust according to respondents. Vast majority of respondents (86%) say that a data breach decreases their trust towards the online service, with only 10% saying that data breach disclosure does not decrease their trust much, and 1% saying there is no impact. The results are in line with real-life examples discussed in chapter 2.2.4, where data breach disclosure have caused significant damage to the reputation of service providers that have been breached. This highlights the importance of service provider paying sufficient amount of attention to the security of the online service, since while there might be no reward for them in terms of data security as long as the data is not breached, the negative impact of potential data breach can be significant.

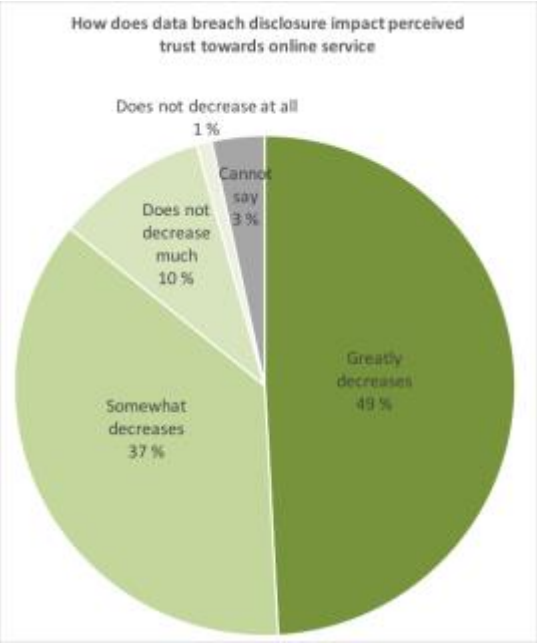

Figure 27

Based on the results, *Hypothesis 12: Data breach disclosures have a negative impact on perceived trust towards online service* is supported**.**

5.4 Usability

Existing research shows that usability impacts the online trust perceived by users, as pointed out in chapter 2.2.5. This chapter discussed the impact of two usability related elements, ease of authentication and availability of online service, on perceived trust towards online service.

5.4.1 Ease of authentication

Impact of ease of authentication on perceived online trust

The impact of ease of authentication on trust was studied by asking the respondents how easy to use they find a specific authentication method, and then asking how does using a specific authentication method for user identification impacts their trust towards online service. The authentication methods included in the survey are Bank-ID authentication, mobile phone authentication biometric authentication and two forms of password authentication: One where the users are allowed to select username and password themselves, and one where the username is generated by the service but users are allowed to select the password themselves. Figure 28 describes perceived ease of use of each authentication method, and figure 29 describes how each authentication method impacts perceived trust towards online service when they are used for identifying the user.

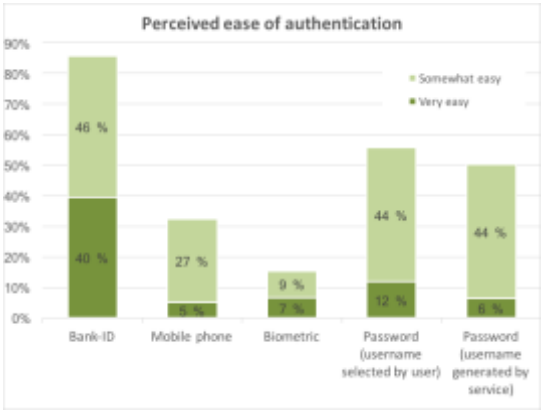

Figure 28

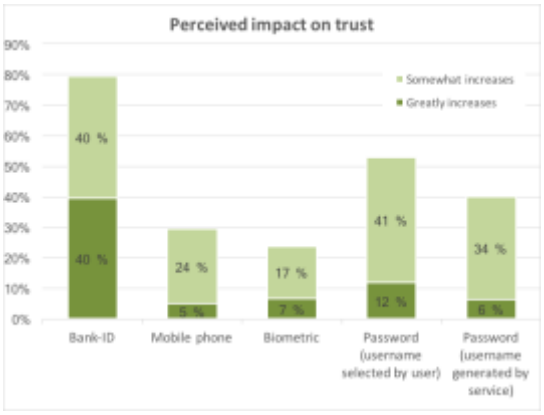

Figure 29

Participants considered Bank-ID the easiest to use, followed by the two password-based authentication methods, mobile phone authentication and biometric authentication. When asked about perceived impact of trust towards the online service, the order was exactly the same: Using Bank-ID for authentication increases the trust towards online service the most, whereas using biometric authentication seems to have the smallest positive impact on perceived trust.

Whether the authentication method used for authentication is considered strong or weak, does not seem to impact perceived trust towards online service, as concluded in chapter 5.2.2. However, there appears to be correlation between perceived ease of use of authentication method, and authentication method's perceived impact on trust. Password authentication as a weaker authentication method is considered easier to use and more trust increasing than stronger authentication methods like mobile phone authentication and biometric authentication.

Regression analysis in figure 30 shows clearly that there is a correlation between perceived ease of use, and perceived impact on trust. The easier to use the authentication method is considered, the more positively it seems to impact trust. The curve that models impact of perceived ease of use on perceived impact on trust seems to be growing exponentially, but no conclusions can be made based on that since only small amount of authentication methods are included in the survey. Nevertheless, the correlation between those two factors included in the survey are clear, and based on that *Hypothesis 13: Easy-to-use authentication method increases perceived trust towards online service* can be concluded as supported.

Figure 30

The results regarding perceived ease of use of different authentication methods also contain some surprises. Bank-ID authentication, that was found easy to use by majority of survey respondents, typically requires a separate PIN-card, and expectation before the survey was conducted was that Bank-ID authentication would not have been considered among easiest authentication methods among respondents. Mobile phone and biometric authentication on the other hand only require a mobile phone, which is something that most correspondents – Finnish citizens – are accustomed to use and presumably usually carry with them anyway. However, mobile phone and biometric authentication was considered the two most difficult authentication methods, as well as least trust increasing authentication methods.

This could be related to personal variables, i.e. how familiar respondents are with different authentication methods. A potential explanation to the results could be that respondents consider authentication methods they have used earlier easier than authentication methods they have used never before. This assumption is supported by differences in results between different respondent groups. Of those respondents, who were classified either as first adopters or digitally active, 49% considered mobile phone authentication easy to use, and 24% of them considered biometric authentication easy to use, whereas corresponding numbers among digitally passive respondents were only 23% and 6%.

5.4.2 Availability

Impact of availability on perceived online trust

Availability refers to a whether the service can be accessed on any given time the user is trying to access it. Figure 31 describes how respondents consider the availability to impact their trust towards the online service. In case the online service is not available when user is trying to access it, the trust towards the service greatly decreases or somewhat decreases according to 50% of the respondents. 44% of respondents say their trust does not decrease much, or does not decrease at all.

With half of the respondents saying the lack of availability decreases their trust towards the online service, *Hypothesis 14: Decreased availability decreases perceived trust towards online service* is supported.

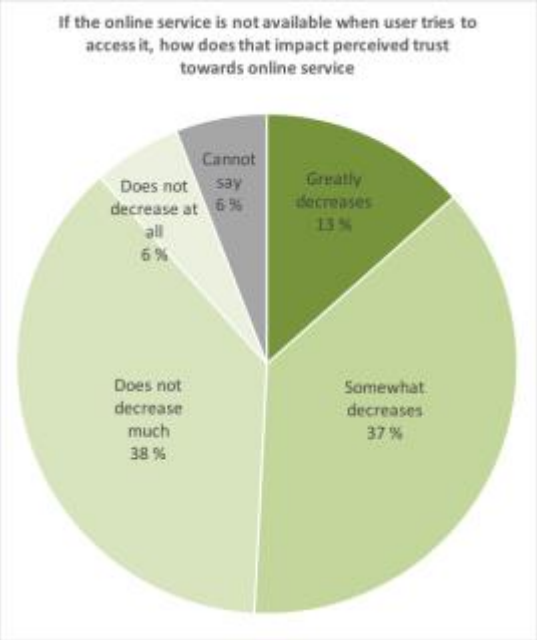

Figure 31

5.5 Findings of the study

Based on the survey results and analysis, hypotheses were either supported, partially supported or not supported. Following table summarizes the findings of the study.

H1: Clear privacy statement / terms of use increases perceived trust towards online service	*supported*
H2: User is more likely to share his or her personal information with online service, if the purpose for which information will be used is communicated to the user in a clear and open manner	*supported*
H3: Control over personal information increases perceived trust towards online service	*supported*
H4: Increased trust towards online service increases the likelihood that a user is willing to share personal information with online service	*supported*
H5: Easy method for sharing personal information increases the likelihood that a user is willing to share personal information with online service	*partially supported*

H6: User is more likely to share personal information with online service, if there is a profit for the user	*supported*
H7: Encrypted transactions increase perceived trust towards online service	*supported*
H8: Using a well-known payment provider for transactions increases perceived trust towards online service	*supported*
H9: Using strong authentication for user identification increases perceived trust towards online service	*not supported*
H10: Security certificate increases perceived trust towards online service	*supported*
H11: The amount that security certificate influences perceived trust depends on user's familiarity with the certificate issuer	*partially supported*
H12: Data breach disclosures have a negative impact on perceived trust towards online service	*supported*
H13: Easy-to-use authentication method increases perceived trust towards online service.	*supported*
H14: Decreased availability decreases perceived trust towards online service.	*supported*

Table 2: Validation of hypotheses

5.6 Discussion of findings

Existing research verifies that online trust is one of the most significant factors influencing purchase intention and customer loyalty of online service users. While there are numerous factors that contribute to the online trust perceived by online service users, privacy, security, reputation and usability are the central elements that impact online trust, and should be considered by every service provider when developing a new online service or upgrading an existing one. There are several ways to increase perceived online trust by paying attention to these elements of trust during online service development process, and on the other hand minimize their potentially negative impact on perceived online trust. This study examined how different approaches to privacy, security and usability impact perceived online trust, and what kind of impact reputational damage due to data breaches can have on perceived online trust.

Privacy is acknowledged as one of the main factors that influence online trust, with transparency and control over personal information being two main privacy issues the service providers should concentrate when designing an online service. In terms of transparency, a clear privacy statement and terms of use increase users' trust towards the online service. Moreover, transparency and openness regarding how the personal information users share with the online service will be used increases users' willingness

to share information with the service.

In terms on control, the study concludes that when users are given control over usage of their personal information, and/or they are allowed to modify or remove the information online service has collected of them, users' trust towards the online service increases. Increased trust, in turn, makes users more willing to share personal information with the service. Another way to increase users' willingness to share personal information is a profit, such as discount or better user experience, in exchange for information they have share with the service. Also, having reasonable limits for the amount of information user is asked to enter at a time seems to increase willingness to share information with the service, whereas fetching users' personal information from a social media service such as Facebook decreases the willingness to share information.

Security is another key factor in building online trust. Encrypted transactions are one key aspect of transaction security, and based on the results of this study most users recognize a situation where the transactions are encrypted, and vast majority of users consider encrypted transactions as a very important factor regarding online service security. Also, using an external payment provider for transactions is recommended, since users find transaction that are made using external payment provider more secure than direct credit card transactions with the online service.

However, using strong authentication for user identification does not appear to increase perceived online trust. User identification by password authentication was considered to increase trust towards the online service more than some strong authentication methods such as mobile phone authentication or biometric authentication. On the other hand, strong authentication by Bank-ID was found to increase perceived trust by vast majority of users, and it had a bigger positive impact on trust than password authentication.

Security certificate confirming that the online service has passed a security audit seems to positively influence online trust. The impact of security certificate also depends on the issuer, as Finnish consumers considers security certificates issued by Finnish companies, or by a company the user knows by name, more trustworthy than certificates issued by foreign companies.

Reputation of the online service and service provider also influence online trust. Based on the results of this study, data breach disclosures can cause significant damage to the reputation of online service, and thus decrease online trust among potential customers. Therefore, service providers should implement proper measures for protecting the data stored within the service, since while there might be no visible reward for data security, the lack of data security can cause major problems in terms of online trust towards the service or service provider.

Usability of the online service also impact perceived trust towards the service. Easy-to-use method for user authentication appears to influence trust perceived by the users.

Vice versa, authentication methods that are difficult to use decrease perceived online trust. Regarding usability, online service should also be available whenever user tries to access it, since interruptions in availability appear to have a negative impact on users' trust towards the online service.

This study concludes that privacy, security, reputation and usability are factors that contribute to the perceived online trust, and thus make online service users more likely to make the initial purchase, and continue using the online service as repeat customers. Findings of this study represent a concrete list of items that service providers can focus on in order to improve or maintain perceived online trust by means of privacy, security and usability practises.

5.7 Limitations of this study

The motivation for the study was to better understand those areas of online service security for which cybersecurity companies could provide services for. Therefore, this study mainly focuses on trust from security perspective, and some of the aspects that contribute to the trust experienced by the user are discussed in this study, but not included in the survey. Some elements that could intuitively affect the trust perceived by the user towards online service, such as look-and-feel of the service, or marketing efforts taken by the service provider in order to enhance its brand image and trustworthiness, are briefly discussed but not the main focus of this study. Because of these limitations, this study should not be interpreted as a comprehensive research covering all the elements that contribute to online trust and thus impact purchase intention and customer loyalty of online service users, but rather a study that indicates what kind of trust-related elements online service providers should consider when developing new online services.

6. Conclusions

Online service business is growing rapidly, and online service providers are looking for new ways to differentiate their online services from competition. Trust perceived by online service users towards the online service has been identified as one of the key factors that influence purchase intention and customer loyalty, which in turn contribute to the success or failure of the online service. The goal of this study was to examine what are the individual items that impact perceived online trust, thus impacting purchase intention and customer loyalty.

A literature review on existing research confirms that online trust is one of the most significant factors that influence purchase intention and customer loyalty of online service users. Existing literature demonstrates privacy, security, reputation and usability as key elements of online trust. In this study, a research model was developed and a survey was conducted in order to examine the correlation between individual items related to those four categories and perceived online trust.

Findings of the study show that online services' openness regarding privacy policies and control given for the users over their personal information make users more likely to trust the online service and share their personal information with the service. Users are also more likely to share information with the service when there are easy methods available for sharing the information, however retrieving user data from social media services appears to decrease willingness to share information with the online service.

In terms of security, the results suggest that using encrypted transactions and trusted external payment providers have a clear positive impact on perceived trust towards the online service, as well as security certificates verifying that the online service has passed a security audit. Using strong authentication for user identification on the other hand does not seem to have a correlation with perceived online trust, whereas ease of authentication appears to positively correlate with perceived online trust.

Data breach disclosures can cause significant reputational damage to the online service, thus decreasing the perceived trust towards the service. Also, decreased availability of the online service decreases users' trust towards the service.

As a conclusion, there are several aspects related to online service privacy, security, reputation and usability that online service providers should take into account when developing a new online service. If the factors that influence online trust are neglected during the online service development process, there will be implications on consumers' initial purchase intention and customer loyalty, which in turn will often determine the success of the online service. This study provides a list of items for online service providers to consider in order to create a thriving online service that is considered trustworthy by its customers.

References

1. US e-commerce sales grow 15.6% in 2016 [Internet]. [cited 2017 Oct 8]. Available from: https://www.digitalcommerce360.com/2017/02/17/us-e-commerce-sales-grow-156-2016/

2. Lu B, Fan W, Zhou M. Social presence, trust, and social commerce purchase intention: An empirical research. Comput Hum Behav. 2016 Mar;56:225–37.

3. Salo J, Karjaluoto H. A conceptual model of trust in the online environment. Online Inf Rev. 2007 Oct 2;31(5):604–21.

4. Chen Y-H, Barnes S. Initial trust and online buyer behaviour. Ind Manag Data Syst. 2007;107(1):21–36.

5. Yoon S-J. The antecedents and consequences of trust in online-purchase decisions. J Interact Mark. 2002 Jan;16(2):47–63.

6. Kim H-W, Xu Y, Gupta S. Which is more important in Internet shopping, perceived price or trust? Electron Commer Res Appl. 2012 May;11(3):241–52.

7. Kong W, Hung Y-TC. Modeling initial and repeat online trust in B2C e-commerce. In: System Sciences, 2006 HICSS'06 Proceedings of the 39th Annual Hawaii International Conference on [Internet]. IEEE; 2006 [cited 2016 Apr 6]. p. 120b–120b. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1579531

8. Mayer RC, Davis JH, Schoorman FD. An Integrative Model of Organizational Trust. Acad Manage Rev. 1995 Jul;20(3):709.

9. Kim DJ, Ferrin DL, Rao HR. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decis Support Syst. 2008 Jan;44(2):544–64.

10. McKnight DH, Choudhury V, Kacmar C. The impact of initial consumer trust on intentions to transact with a web site: a trust building model. J Strateg Inf Syst. 2002;11(3):297–323.

11. Choon Ling K, Bin Daud D, Hoi Piew T, Keoy KH, Hassan P. Perceived Risk, Perceived Technology, Online Trust for the Online Purchase Intention in Malaysia. Int J Bus Manag [Internet]. 2011 Jun 1 [cited 2016 Apr 6];6(6). Available from: http://www.ccsenet.org/journal/index.php/ijbm/article/view/10825

12. Hwang Y, Lee KC. Investigating the moderating role of uncertainty avoidance cultural values on multidimensional online trust. Inf Manage. 2012 May;49(3–4):171–6.

13. Ganguly B, Dash SB, Cyr D. Website characteristics, Trust and purchase intention in online stores:-An Empirical study in the Indian context. J Inf Sci Technol. 2009;6(2):22–44.

14. Consumer Trust in an Internet Store: A Cross-Cultural Validation - Jarvenpaa - 1999 - Journal of Computer-Mediated Communication - Wiley Online Library [Internet]. [cited 2017 Oct 6]. Available from: http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.1999.tb00337.x/full

15. Kim H-W, Xu Y, Koh J. A comparison of online trust building factors between potential customers and repeat customers. J Assoc Inf Syst. 2004;5(10):13.

16. Flavián C, Guinalíu M. Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. Ind Manag Data Syst. 2006 Jun;106(5):601–20.

17. Harris LC, Goode MM. The four levels of loyalty and the pivotal role of trust: a study of online service dynamics. J Retail. 2004 Jan;80(2):139–58.

18. Lauer TW, Deng X. Building online trust through privacy practices. Int J Inf Secur. 2007 Aug 15;6(5):323–31.

19. Henriksen T. The importance of emotional awareness in business development; When trust becomes a currency [Internet] [Master Thesis in Interaction Design]. The Oslo School of Architecture and Design; 2015 [cited 2017 Apr 8]. Available from: http://theodorhenriksen.com/project/master-thesis-designing-for-trust/

20. Awad NF, Ragowsky A. Establishing Trust in Electronic Commerce Through Online Word of Mouth: An Examination Across Genders. J Manag Inf Syst. 2008 Apr 1;24(4):101–21.

21. Hoffman DL, Novak TP, Peralta M. Building consumer trust online. Commun ACM. 1999;42(4):80–85.

22. Bart Y, Shankar V, Sultan F, Urban GL. Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study. J Mark. 2005 Oct;69(4):133–52.

23. Koufaris M, Hampton-Sosa W. The development of initial trust in an online company by new customers. Inf Manage. 2004 Jan;41(3):377–97.

24. Pan Y, Zinkhan GM. Exploring the impact of online privacy disclosures on consumer trust. J Retail. 2006 Jan;82(4):331–8.

25. Aïmeur E, Lawani O, Dalkir K. When changing the look of privacy policies affects user trust: An experimental study. Comput Hum Behav. 2016 May;58:368–79.

26. Sofres TN. Global e-commerce report 2002. June Tnsofres ComGeR2002 [Internet]. 2002 [cited 2017 Oct 6]; Available from: http://www.tns-nipo.com/pages/persvannipo/pdf/rapport_ger2002.pdf

27. Kim C, Tao W, Shin N, Kim K-S. An empirical study of customers' perceptions of security and trust in e-payment systems. Electron Commer Res Appl. 2010 Jan;9(1):84–95.

28. PayPal: annual revenue 2016 | Statistic [Internet]. [cited 2017 Oct 15]. Available from: https://www.statista.com/statistics/382619/paypal-annual-revenue/

29. Zhang D, Ma Z, Niu X, Peng Y. Anonymous authentication scheme of trusted mobile terminal under mobile Internet. J China Univ Posts Telecommun. 2013 Feb;20(1):58–65.

30. Hu X, Lin Z, Zhang H. Myth or reality: Effect of trust-promoting seals in electronic markets. Trust Netw Econ. 2003;143–150.

31. Edelman B, others. Adverse Selection in Online 'Trust' Certifications. In: WEIS [Internet]. Citeseer; 2006 [cited 2016 Apr 6]. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.137.2417&rep=rep1&type=pdf

32. Culnan MJ, Williams CC. How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. Mis Q. 2009;673–687.

33. Everard A, Galletta DF. How presentation flaws affect perceived site quality, trust, and intention to purchase from an online store. J Manag Inf Syst. 2005;22(3):56–95.

34. Gregg DG, Walczak S. The relationship between website quality, trust and price premiums at online auctions. Electron Commer Res. 2010 Mar;10(1):1–25.

35. Parasuraman A, Zeithaml VA, Malhotra A. E-S-QUAL: A Multiple-Item Scale for Assessing Electronic Service Quality. J Serv Res. 2005 Feb;7(3):213–33.

36. Dickinger A, Stangl B. Website performance and behavioral consequences: A formative measurement approach. J Bus Res. 2013 Jun;66(6):771–7.

Appendix 1: Summary of survey results

Survey results including all responses (N=779), presented with 95% confidence interval.

Transparency

If privacy statement / terms of use of the online service are clear and easy-to-understand, how does that impact perceived trust towards online service

	(%)	95% CI
Greatly increases	47,9	± 3,4
Somewhat increases	37,9	± 3,4
Does not increase much	8,1	± 2,1
Does not increase at all	1,6	± 1,5
Cannot say	4,6	± 1,5

If the purpose for which personal information will be used is communicated in a clear and open manner, how does that impact willingness to share personal information with the online service

	(%)	95% CI
Greatly increases	19,5	± 2,8
Somewhat increases	49,0	± 3,4
Does not increase or decrease	23,3	± 2,8
Somewhat decreases	3,3	± 1,5
Greatly decreases	2,4	± 1,5
Cannot say	2,4	± 1,5

Control

If user is allowed to control to which purpose user's personal information will be used, how does that impact perceived trust towards online service

	(%)	95% CI
Greatly increases	65,2	± 3,3
Somewhat increases	26,7	± 3,0
Does not increase or decrease	4,7	± 1,5

Decreases	0,4	± 1,5
Cannot say	3,1	± 1,5

If user is allowed to modify or remove personal information, how does that impact perceived trust towards online service

	(%)	95% CI
Greatly increases	58,5	± 3,3
Somewhat increases	30,2	± 3,2
Does not increase or decrease	6,1	± 1,5
Decreases	0,9	± 1,5
Cannot say	4,3	± 1,5

When perceived trust towards online service increases, willingness to share personal information with the online service increases

	(%)	95% CI
Strongly agree	5,0	± 1,5
Somewhat agree	42,3	± 3,4
Do not agree or disagree	21,2	± 2,8
Somewhat disagree	19,6	± 2,8
Strongly disagree	8,7	± 2,1
Cannot say	3,1	± 1,5

If the amount of personal information that needs to be shared with online service at a time is reasonably limited, how does that impact willingness to share personal information with the online service

	(%)	95% CI
Greatly increases	2,8	± 1,5
Somewhat increases	37,4	± 3,3
Does not increase or decrease	42,7	± 3,4
Somewhat decreases	7,7	± 2,1
Greatly decreases	4,8	± 1,5
Cannot say	4,6	± 1,5

If personal information does not need to be typed in by user but online service gets it from a social media service instead, how does that impact willingness to share personal information with the online service

	(%)	95% CI
Greatly increases	1,4	± 1,5
Somewhat increases	13,2	± 2,5
Does not increase or decrease	31,5	± 3,2
Somewhat decreases	21,8	± 2,8
Greatly decreases	27,2	± 3,0
Cannot say	5,0	± 1,5

If there is a profit (e.g. discount) for the user, willingness to share personal information with the online service increases

	(%)	95% CI
Strongly agree	3,4	± 1,5
Somewhat agree	29,9	± 3,2
Do not agree or disagree	22,0	± 2,8
Somewhat disagree	28,6	± 3,2
Strongly disagree	13,5	± 2,5
Cannot say	2,6	± 1,5

If the user would receive better end user experience based on information shared with the online service, how does that impact willingness to share personal information with the online service

	(%)	95% CI
Greatly increases	3,5	± 1,5
Somewhat increases	35,3	± 3,3
Does not increase or decrease	41,4	± 3,4
Somewhat decreases	10,1	± 2,1
Greatly decreases	5,9	± 1,5
Cannot say	3,8	± 1,5

Transaction security

User recognizes a situation where transactions with the online service are encrypted

	(%)	95% CI
Yes	72,8	± 3,0

No	14,8	± 2,5
Cannot say	12,4	± 2,1

How important are encrypted transactions with the online service are in terms of transaction security

	(%)	95% CI
Very important	65,3	± 3,3
Somewhat important	28,8	± 3,2
Not very important	3,2	± 1,5
Not important at all	0,3	± 1,5
Cannot say	2,4	± 1,5

How secure do users consider transactions that are made by online bank payment

	(%)	95% CI
Very secure	38,5	± 3,4
Somewhat secure	51,8	± 3,5
Not secure or insecure	4,7	± 1,5
Somewhat insecure	3,2	± 1,5
Very insecure	0,4	± 1,5
Cannot say	1,3	± 1,5

How secure do users consider transactions that are made via Nordic payment provider (e.g. Klarna)

	(%)	95% CI
Very secure	16,9	± 2,5
Somewhat secure	38,1	± 3,4
Not secure or insecure	18,4	± 2,8
Somewhat insecure	5	± 1,5
Very insecure	1,5	± 1,5
Cannot say	20,1	± 2,8

How secure do users consider transactions that are made via international payment provider (e.g. PayPal)

	(%)	95% CI

Very secure	11,7	± 2,1
Somewhat secure	36	± 3,3
Not secure or insecure	22,6	± 2,8
Somewhat insecure	9,7	± 2,1
Very insecure	2,2	± 1,5
Cannot say	17,8	± 2,8

How secure do users consider transactions that are made directly with the online service (e.g. credit card number is provided for the online service)

	(%)	95% CI
Very secure	3,5	± 1,5
Somewhat secure	18,3	± 2,8
Not secure or insecure	32	± 3,2
Somewhat insecure	27,3	± 3,0
Very insecure	11,7	± 1,5
Cannot say	7,2	± 1,5

Authentication level

If the authentication is made with Bank-ID, how does that impact perceived trust towards online service

	(%)	95% CI
Greatly increases	39,5	± 3,4
Somewhat increases	40,0	± 3,4
Does not increase or decrease	12,7	± 2,5
Somewhat decreases	2,8	± 1,5
Greatly decreases	1,3	± 1,5
Cannot say	3,7	± 1,5

If the authentication is made with mobile phone, how does that impact perceived trust towards online service

	(%)	95% CI
Greatly increases	5,1	± 1,5
Somewhat increases	24,3	± 3,0
Does not increase or decrease	38,7	± 3,4

Somewhat decreases	12,4	± 2,1
Greatly decreases	5,8	± 1,5
Cannot say	13,8	± 2,5

If the authentication is made with biometric authentication (e.g. with laptop or mobile phone camera), how does that impact perceived trust towards online service

	(%)	95% CI
Greatly increases	6,7	± 1,5
Somewhat increases	17,1	± 2,8
Does not increase or decrease	32,9	± 3,2
Somewhat decreases	9,4	± 2,1
Greatly decreases	9,5	± 2,1
Cannot say	24,4	± 3,0

If the authentication is made with username and password created by the user, how does that impact perceived trust towards online service

	(%)	95% CI
Greatly increases	11,9	± 2,1
Somewhat increases	40,9	± 3,4
Does not increase or decrease	37,9	± 3,4
Somewhat decreases	2,8	± 1,5
Greatly decreases	1,2	± 1,5
Cannot say	5,2	± 1,5

Security certifications

If the online service has received a security certificate for passing a security audit, does that increase trust towards the online service

	(%)	95% CI
Yes	53,3	± 3,4
No	22,1	± 2,8
Cannot say	24,6	± 3,0

If which of the following cases does certificate positively impact on trust towards online service

	(%)	95% CI
Certificate has been issued by Finnish company	36,7	± 3,3
Certificate has been issued by foreign company	9,2	± 2,1
Certificate has been issued by a company user knows by name	23,7	± 3,0
Other / cannot say	1,4	± 1,5

Data breach disclosures

How does data breach disclosure impact perceived trust towards online service

	(%)	95% CI
Greatly decreases	49,2	± 3,5
Somewhat decreases	36,7	± 3,3
Does not decrease much	9,8	± 2,1
Does not decrease at all	1,0	± 1,5
Cannot say	3,4	± 1,5

Ease of authentication

How easy to use is Bank-ID authentication

	(%)	95% CI
Very easy	33,7	± 3,2
Somewhat easy	46,2	± 3,4
Not easy or difficult	10,4	± 2,1
Somewhat difficult	6,0	± 1,5
Very difficult	1,6	± 1,5
Cannot say	2,1	± 1,5

How easy to use is mobile phone authentication

	(%)	95% CI
Very easy	8,8	± 2,1
Somewhat easy	27,3	± 3,0
Not easy or difficult	22,6	± 3,0
Somewhat difficult	17,3	± 2,5
Very difficult	6,6	± 1,5
Cannot say	17,4	± 2,8

How easy to use is biometric authentication (e.g. with laptop or mobile phone camera)

	(%)	95% CI
Very easy	3,1	± 1,5
Somewhat easy	8,7	± 2,1
Not easy or difficult	18,6	± 2,8
Somewhat difficult	18,9	± 2,8
Very difficult	20,3	± 2,8
Cannot say	30,4	± 3,2

How easy to user is password authentication (username and password selected by the user)

	(%)	95% CI
Very easy	30,6	± 3,2
Somewhat easy	43,8	± 3,4
Not easy or difficult	14,4	± 2,5
Somewhat difficult	7,1	± 1,5
Very difficult	1,3	± 1,5
Cannot say	2,7	± 1,5

How easy to user is password authentication (username generated by the service, password selected by the user)

	(%)	95% CI
Very easy	19,5	± 2,8
Somewhat easy	43,8	± 3,4
Not easy or difficult	17,9	± 2,8
Somewhat difficult	12,7	± 2,5
Very difficult	2,5	± 1,5
Cannot say	3,7	± 1,5

If the authentication is made with Bank-ID, how does that impact perceived trust towards online service

	(%)	95% CI

Greatly increases	39,5	± 3,4
Somewhat increases	40,0	± 3,4
Does not increase or decrease	12,7	± 2,5
Somewhat decreases	2,8	± 1,5
Greatly decreases	1,3	± 1,5
Cannot say	3,7	± 1,5

If the authentication is made with mobile phone, how does that impact perceived trust towards online service

	(%)	95% CI
Greatly increases	5,1	± 1,5
Somewhat increases	24,3	± 3,0
Does not increase or decrease	38,7	± 3,4
Somewhat decreases	12,4	± 2,1
Greatly decreases	5,8	± 1,5
Cannot say	13,8	± 2,8

If the authentication is made with biometric authentication (e.g. with laptop or mobile phone camera), how does that impact perceived trust towards online service

	(%)	95% CI
Greatly increases	6,7	± 1,5
Somewhat increases	17,1	± 2,8
Does not increase or decrease	32,9	± 3,2
Somewhat decreases	9,4	± 2,1
Greatly decreases	9,5	± 2,1
Cannot say	24,4	± 3,0

If the authentication is made with username and password selected by the user, how does that impact perceived trust towards online service

	(%)	95% CI
Greatly increases	11,9	± 2,1
Somewhat increases	40,9	± 3,4
Does not increase or decrease	37,9	± 3,4
Somewhat decreases	2,8	± 1,5
Greatly decreases	1,2	± 1,5
Cannot say	5,2	± 1,5

If the authentication is made with username generated by the service, and password selected by the user, how does that impact perceived trust towards online service

	(%)	95% CI
Greatly increases	6,4	± 1,5
Somewhat increases	33,7	± 3,3
Does not increase or decrease	45,6	± 3,4
Somewhat decreases	7,2	± 1,5
Greatly decreases	1,5	± 1,5
Cannot say	5,7	± 1,5

Availability

If the online service is not available when user tries to access it, how does that impact perceived trust towards online service

	(%)	95% CI
Greatly decreases	13,4	± 2,5
Somewhat decreases	37,4	± 3,3
Does not decrease much	37,6	± 3,4
Does not decrease at all	5,7	± 1,5
Cannot say	5,9	± 1,5